(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－234728
（P2003－234728A）
(43)公開日　平成15年８月22日(2003.8.22)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０		３２０Ｆ	５Ｊ１０４
		Ｈ０４Ｌ　9/00	６０１Ｂ	
Ｈ０４Ｌ　9/32			６０１Ａ	
			６７５Ｂ	

審査請求　未請求　請求項の数83　ＯＬ　（全 45 頁）　最終頁に続く

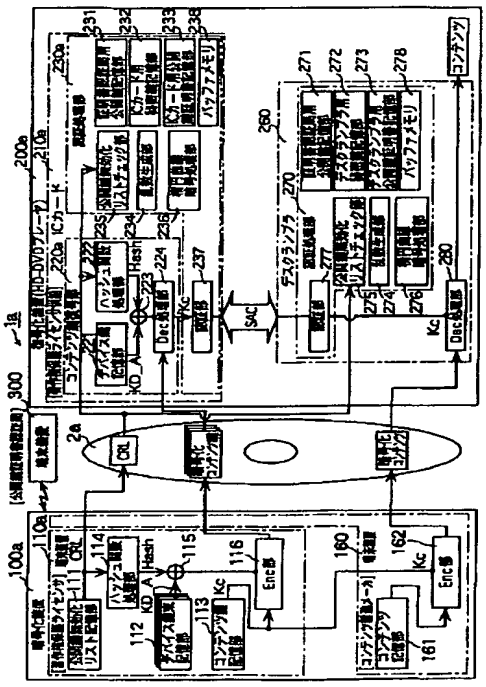
(21)出願番号　特願2002－259514(P2002－259514)
(22)出願日　平成14年９月５日(2002.9.5)
(31)優先権主張番号　特願2001－298414(P2001－298414)
(32)優先日　平成13年９月27日(2001.9.27)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願2001－374856(P2001－374856)
(32)優先日　平成13年12月７日(2001.12.7)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　大森　基司
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100109210
弁理士　新居　広守

最終頁に続く

(54)【発明の名称】　暗号化装置、復号化装置、秘密鍵生成装置、著作権保護システムおよび暗号通信装置

(57)【要約】
【課題】　公開鍵証明書無効化リストの差し替え攻撃に対して防御することができ、安全にデジタル著作物を転送する暗号化装置を提供する。
【解決手段】　公開鍵証明書無効化リストを記憶する公開鍵無効化リスト記憶部１１１と、復号化装置２００ａで用いられるＩＣカード２１０ａごとに固有のデバイス鍵ＫＤ＿Ａを記憶するデバイス鍵束記憶部１１２と、コンテンツを暗号化するための秘密鍵であるコンテンツ鍵Ｋｃを記憶するコンテンツ鍵記憶部１１３と、ハッシュ関数にしたがって公開鍵無効化リスト記憶部１１１に記憶された公開鍵証明書無効化リストのハッシュ値を算出するハッシュ関数処理部１１４と、そのハッシュ値とデバイス鍵ＫＤ＿Ａとの排他的論理和をとるＥｘ－ＯＲ部１１５と、コンテンツ鍵ＫｃをＥｘ－ＯＲ部１１５の出力値で暗号化するＥｎｃ部１１６とを備える。



BEST AVAILABLE COPY

1

【特許請求の範囲】

【請求項１】　デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、

デジタル著作物を記憶するデジタル著作物記憶手段と、

デジタル著作物の暗号化に用いられる第１秘密鍵を記憶する第１秘密鍵記憶手段と、

暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第２秘密鍵を記憶する第２秘密鍵記憶手段と、

無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、

前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記第２秘密鍵記憶手段に記憶された第２秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記変形手段により変形された第２秘密鍵で暗号化する第１暗号化手段と、

前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記第１秘密鍵記憶手段に記憶された第１秘密鍵で暗号化する第２暗号化手段と、

前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第１暗号化手段により暗号化された第１秘密鍵および前記第２暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

【請求項２】　前記暗号化装置は、さらに、

前記復号化装置において復号化された第１秘密鍵が正しいものであるか否かを確認するための基準となる確認データを前記記録媒体又は伝送媒体に出力する確認データ出力手段を備えることを特徴とする請求項１記載の暗号化装置。

【請求項３】　前記確認データ出力手段は、所定の固定パターンのデータを前記第１秘密鍵記憶手段に記憶された第１秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力することを特徴とする請求項２記載の暗号化装置。

【請求項４】　前記確認データ出力手段は、前記第１秘密鍵記憶手段に記憶された第１秘密鍵を当該第１秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力することを特徴とする請求項２記載の暗号化装置。

【請求項５】　前記属性値算出手段は、前記公開鍵無効化リストのハッシュ値を前記属性値として算出し、

前記変形手段は、前記第２秘密鍵と前記ハッシュ値との排他的論理和をとることによって、前記第２秘密鍵を変形させることを特徴とする請求項１記載の暗号化装置。

2

【請求項６】　デジタル著作物であるデジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、

デジタル著作物を記憶するデジタル著作物記憶手段と、

デジタル著作物の暗号化に用いられる第１秘密鍵を記憶する第１秘密鍵記憶手段と、

暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第２秘密鍵を記憶する第２秘密鍵記憶手段と、

無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、

前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記第２秘密鍵記憶手段に記憶された第２秘密鍵で暗号化する第１暗号化手段と、

前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記変形手段により変形された第１秘密鍵で暗号化する第２暗号化手段と、

前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第１暗号化手段により暗号化された第１秘密鍵および前記第２暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

【請求項７】　前記暗号化装置は、さらに、

前記復号化装置において復号化された第１秘密鍵が正しいものであるか否かを確認するための基準となる確認データを前記記録媒体又は伝送媒体に出力する確認データ出力手段を備えることを特徴とする請求項６記載の暗号化装置。

【請求項８】　前記確認データ出力手段は、所定の固定パターンのデータを前記変形手段で変形された第１秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力することを特徴とする請求項７記載の暗号化装置。

【請求項９】　前記確認データ出力手段は、前記変形手段で変形された第１秘密を当該第１秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力することを特徴とする請求項７記載の暗号化装置。

【請求項１０】　デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、

デジタル著作物を記憶するデジタル著作物記憶手段と、

デジタル著作物の暗号化に用いられる媒体識別情報を記憶する媒体識別情報記憶手段と、

暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第１秘密鍵を記憶する第１秘密鍵記憶手段と、

無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、

前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記媒体識別情報記憶手段に記憶された媒体識別情報と前記変形手段で変形された第１秘密鍵とを一方向性関数に入力して変換する関数変換手段と、

前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記関数変換手段で得られた関数値で暗号化する第２暗号化手段と、

前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記媒体識別情報記憶手段に記憶された媒体識別情報および前記第２暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

【請求項１１】　デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、

デジタル著作物を記憶するデジタル著作物記憶手段と、

デジタル著作物の暗号化に用いられる媒体識別情報を記憶する媒体識別情報記憶手段と、

暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第１秘密鍵を記憶する第１秘密鍵記憶手段と、

無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、

前記媒体識別情報記憶手段に記憶された媒体識別情報と前記第１秘密鍵記憶手段に記憶された第１秘密鍵とを一方向性関数に入力して変換する関数変換手段と、

前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記関数変換手段で得られた関数値を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記変形手段で変形された属性値で暗号化する第１暗号化手段と、

前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記媒体識別情報記憶手段に記憶された媒体識別情報および前記第１暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

【請求項１２】　デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、

デジタル著作物を記憶するデジタル著作物記憶手段と、

デジタル著作物の暗号化に用いられる第１秘密鍵を記憶する第１秘密鍵記憶手段と、

暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第２秘密鍵を記憶する第２秘密鍵記憶手段と、

前記第１秘密鍵の暗号化に用いられる第３秘密鍵を記憶する第３秘密鍵記憶手段と、

無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、

前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記第２秘密鍵記憶手段に記憶された第２秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記第３秘密鍵記憶手段に記憶された第３秘密鍵を前記変形手段により変形された第２秘密鍵で暗号化する第１暗号化手段と、

前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記第３秘密鍵記憶手段に記憶された第３秘密鍵で暗号化する第２暗号化手段と、

前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記第１秘密鍵記憶手段に記憶された第１秘密鍵で暗号化する第３暗号化手段と、

前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第１暗号化手段により暗号化された第３秘密鍵、前記第２暗号化手段により暗号化された第１秘密鍵および前記第３暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

【請求項１３】　前記暗号化装置は、さらに、

前記復号化装置において復号化された第３秘密鍵が正しいものであるか否かを確認するための基準となる確認データを前記記録媒体又は伝送媒体に出力する確認データ出力手段を備えることを特徴とする請求項１２記載の暗号化装置。

【請求項１４】　前記確認データ出力手段は、所定の固定パターンのデータを前記第３秘密鍵記憶手段に記憶された第３秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力することを特徴とする請求項１３記載の暗号化装置。

【請求項１５】　前記確認データ出力手段は、前記第３秘密鍵記憶手段に記憶された第３秘密鍵を当該第３秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力することを特徴とする請求項１３記載の暗号化装置。

5

【請求項１６】　デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、
デジタル著作物を記憶するデジタル著作物記憶手段と、
デジタル著作物の暗号化に用いられる第１秘密鍵を記憶する第１秘密鍵記憶手段と、
暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第２秘密鍵を記憶する第２秘密鍵記憶手段と、
前記第１秘密鍵の暗号化に用いられる第３秘密鍵を記憶する第３秘密鍵記憶手段と、
無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、
前記第３秘密鍵記憶手段に記憶された第３秘密鍵を前記第２秘密鍵記憶手段に記憶された第２秘密鍵で暗号化する第１暗号化手段と、
前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記第３秘密鍵記憶手段に記憶された第３秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、
前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記変形手段で変形された属性値で暗号化する第２暗号化手段と、
前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記第１秘密鍵記憶手段に記憶された第１秘密鍵で暗号化する第３暗号化手段と、
前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第１暗号化手段により暗号化された第３秘密鍵、前記第２暗号化手段により暗号化された第１秘密鍵および前記第３暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。
【請求項１７】　デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、
デジタル著作物を記憶するデジタル著作物記憶手段と、
デジタル著作物の暗号化に用いられる第１秘密鍵を記憶する第１秘密鍵記憶手段と、
暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第２秘密鍵を記憶する第２秘密鍵記憶手段と、
前記第１秘密鍵の暗号化に用いられる第３秘密鍵を記憶する第３秘密鍵記憶手段と、
無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、
前記第３秘密鍵記憶手段に記憶された第３秘密鍵を前記第２秘密鍵記憶手段に記憶された第２秘密鍵で暗号化する第１暗号化手段と、

6

前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記第１暗号化手段で暗号化された第３秘密鍵で暗号化する第２暗号化手段と、
前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、
前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記変形手段で変形された第１秘密鍵で暗号化する第３暗号化手段と、
前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第１暗号化手段により暗号化された第３秘密鍵、前記第２暗号化手段により暗号化された第１秘密鍵および前記第３暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。
【請求項１８】　デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、
デジタル著作物を記憶するデジタル著作物記憶手段と、
デジタル著作物の暗号化に用いられる媒体識別情報を記憶する媒体識別情報記憶手段と、
暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第１秘密鍵を記憶する第１秘密鍵記憶手段と、
前記媒体識別情報の暗号化に用いられる第２秘密鍵を記憶する第２秘密鍵記憶手段と、
無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、
前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、
前記第２秘密鍵記憶手段に記憶された第２秘密鍵を前記変形手段により変形された第１秘密鍵で暗号化する第１暗号化手段と、
前記媒体識別情報記憶手段に記憶された媒体識別情報と前記第２秘密鍵記憶手段に記憶された第２秘密鍵とを一方向性関数に入力して変換する関数変換手段と、
前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記関数変換手段で得られた関数値で暗号化する第２暗号化手段と、
前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第１暗号化手段により暗号化された第２秘密鍵、前記媒体識別情報記憶手段に記憶された媒体識別情報および前記第３暗号化手段により暗号化された

デジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

【請求項１９】　前記暗号化装置は、さらに、

前記復号化装置において復号化された第２秘密鍵が正しいものであるか否かを確認するための基準となる確認データを前記記録媒体又は伝送媒体に出力する確認データ出力手段を備えることを特徴とする請求項１８記載の暗号化装置。

【請求項２０】　前記確認データ出力手段は、所定の固定パターンのデータを前記第２秘密鍵記憶手段に記憶された第２秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力することを特徴とする請求項１９記載の暗号化装置。

【請求項２１】前記確認データ出力手段は、前記第２秘密鍵記憶手段に記憶された第２秘密鍵を当該第２秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力することを特徴とする請求項１９記載の暗号化装置。

【請求項２２】　デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、

デジタル著作物を記憶するデジタル著作物記憶手段と、

デジタル著作物の暗号化に用いられる媒体識別情報を記憶する媒体識別情報記憶手段と、

暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第１秘密鍵を記憶する第１秘密鍵記憶手段と、

前記媒体識別情報の暗号化に用いられる第２秘密鍵を記憶する第２秘密鍵記憶手段と、

無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、

前記第２秘密鍵記憶手段に記憶された第２秘密鍵を前記第１秘密鍵記憶手段に記憶された第１秘密鍵で暗号化する第１暗号化手段と、

前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記第２秘密鍵記憶手段に記憶された第２秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記媒体識別情報記憶手段に記憶された媒体識別情報と前記変形手段で変形された第２秘密鍵とを一方向性関数に入力して変換する関数変換手段と、

前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記関数変換手段で得られた関数値で暗号化する第２暗号化手段と、

前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第１暗号化手段により暗号化された第２秘密鍵、前記媒体識別情報記憶手段に記憶された媒体識別情報および前記第３暗号化手段により暗号化された

デジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

【請求項２３】　デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、

デジタル著作物を記憶するデジタル著作物記憶手段と、

デジタル著作物の暗号化に用いられる媒体識別情報を記憶する媒体識別情報記憶手段と、

暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第１秘密鍵を記憶する第１秘密鍵記憶手段と、

前記媒体識別情報の暗号化に用いられる第２秘密鍵を記憶する第２秘密鍵記憶手段と、

無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、

前記第２秘密鍵記憶手段に記憶された第２秘密鍵を前記第１秘密鍵記憶手段に記憶された第１秘密鍵で暗号化する第１暗号化手段と、

前記媒体識別情報記憶手段に記憶された媒体識別情報と前記第２秘密鍵記憶手段に記憶された第２秘密鍵とを一方向性関数に入力して変換する関数変換手段と、

前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記関数変換手段で得られた関数値を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記変形手段で変形された関数値で暗号化する第２暗号化手段と、

前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第１暗号化手段により暗号化された第２秘密鍵、前記媒体識別情報記憶手段に記憶された媒体識別情報および前記第２暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

【請求項２４】　記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、

暗号化されたデジタル著作物、その暗号化に用いられた第１秘密鍵を暗号化した暗号化第１秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、

当該復号化装置に固有の第２秘密鍵を記憶する第２秘密鍵記憶手段と、

取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記第２秘密鍵記憶手段に記憶された第２秘密鍵を前記属性値算出手段により算出された属性値で変形させる変

形手段と、
前記取得手段により取得された暗号化第１秘密鍵を前記変形手段により変形された第２秘密鍵で復号化する第１復号化手段と、
前記取得手段により取得された暗号化デジタル著作物を前記第１復号化手段により復号化された第１秘密鍵で復号化する第２復号化手段とを備えることを特徴とする復号化装置。
【請求項２５】　前記属性値算出手段は、前記公開鍵無効化リストのハッシュ値を前記属性値として算出し、
前記変形手段は、前記第２秘密鍵と前記ハッシュ値との排他的論理和をとることによって、前記第２秘密鍵を変形させることを特徴とする請求項２４記載の復号化装置。
【請求項２６】　記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、
暗号化されたデジタル著作物、その暗号化に用いられた第１秘密鍵を暗号化した暗号化第１秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、
当該復号化装置に固有の第２秘密鍵を記憶する第２秘密鍵記憶手段と、
前記取得手段により取得された暗号化第１秘密鍵を前記第２秘密鍵記憶手段に記憶された第２秘密鍵で復号化する第１復号化手段と、
前記取得手段に取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記第１復号化手段により復号化された第１秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、
前記取得手段により取得された暗号化デジタル著作物を前記変形手段で変形された第１秘密鍵で復号化する第２復号化手段とを備えることを特徴とする復号化装置。
【請求項２７】　記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、
暗号化されたデジタル著作物、その暗号化に用いられた媒体識別情報および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、
当該復号化装置に固有の第１秘密鍵を記憶する第１秘密鍵記憶手段と、
取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記属性値算出手段により算出された属性値で変形させる変

形手段と、
前記取得手段により取得された媒体識別情報と前記変形手段により変形された第１秘密鍵とを一方向性関数に入力して変換する関数変換手段と、
前記取得手段により取得された暗号化デジタル著作物を前記関数変換手段で得られた関数値で復号化する第１復号化手段とを備えることを特徴とする復号化装置。
【請求項２８】　記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、
暗号化されたデジタル著作物、その暗号化に用いられた媒体識別情報および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、
当該復号化装置に固有の第１秘密鍵を記憶する第１秘密鍵記憶手段と、
前記取得手段により取得された媒体識別情報と前記第１秘密鍵記憶手段に記憶された第１秘密鍵とを一方向性関数に入力して変換する関数変換手段と、
取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記関数変換手段で得られた関数値を前記属性値算出手段により算出された属性値で変形させる変形手段と、
前記取得手段により取得された暗号化デジタル著作物を前記変形手段で変形された属性値で復号化する第１復号化手段とを備えることを特徴とする復号化装置。
【請求項２９】　記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、
暗号化されたデジタル著作物、その暗号化に用いられた第１秘密鍵を暗号化した暗号化第１秘密鍵、前記第１秘密鍵の暗号化に用いられた第２秘密鍵を暗号化した暗号化第２秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、
当該復号化装置に固有の第３秘密鍵を記憶する第３秘密鍵記憶手段と、
取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記第３秘密鍵記憶手段に記憶された第３秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、
前記取得手段により取得された暗号化第２秘密鍵を前記変形手段により変形された第３秘密鍵で復号化する第１復号化手段と、
前記取得手段により取得された暗号化第１秘密鍵を前記第１復号化手段により復号化された第２秘密鍵で復号化する第２復号化手段と、

前記取得手段により取得された暗号化デジタル著作物を前記第２復号化手段により復号化された第１秘密鍵で復号化する第３復号化手段とを備えることを特徴とする復号化装置。

【請求項３０】　記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、

暗号化されたデジタル著作物、その暗号化に用いられた第１秘密鍵を暗号化した暗号化第１秘密鍵、前記第１秘密鍵の暗号化に用いられた第２秘密鍵を暗号化した暗号化第２秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、

当該復号化装置に固有の第３秘密鍵を記憶する第３秘密鍵記憶手段と、

前記取得手段により取得された暗号化第２秘密鍵を前記第３秘密鍵記憶手段に記憶された第３秘密鍵で復号化する第１復号化手段と、

取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記第１復号化手段で復号された第２秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記取得手段により取得された暗号化第１秘密鍵を前記変形手段により変形された第２秘密鍵で復号化する第２復号化手段と、

前記取得手段により取得された暗号化デジタル著作物を前記第２復号化手段により復号化された第１秘密鍵で復号化する第３復号化手段とを備えることを特徴とする復号化装置。

【請求項３１】　記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、

暗号化されたデジタル著作物、その暗号化に用いられた第１秘密鍵を暗号化した暗号化第１秘密鍵、前記第１秘密鍵の暗号化に用いられた第２秘密鍵を暗号化した暗号化第２秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、

当該復号化装置に固有の第３秘密鍵を記憶する第３秘密鍵記憶手段と、

前記取得手段により取得された暗号化第２秘密鍵を前記第１秘密鍵記憶手段に記憶された第３秘密鍵で復号化する第１復号化手段と、

前記取得手段により取得された暗号化第１秘密鍵を前記第１復号化手段により復号化された第２秘密鍵で復号化する第２復号化手段と、

取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値

算出手段と、

前記第２復号化手段により復号化された第１秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記取得手段により取得された暗号化デジタル著作物を前記変形手段により変形された第１秘密鍵で復号化する第３復号化手段とを備えることを特徴とする復号化装置。

【請求項３２】　記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、

暗号化されたデジタル著作物、その暗号化に用いられた媒体識別情報、前記媒体識別情報の暗号化に用いられた第１秘密鍵を暗号化した暗号化第１秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、

当該復号化装置に固有の第２秘密鍵を記憶する第２秘密鍵記憶手段と、

取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記第２秘密鍵記憶手段に記憶された第２秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記取得手段により取得された暗号化第１秘密鍵を前記変形手段により変形された第２秘密鍵で復号化する第１復号化手段と、

前記取得手段により取得された媒体識別情報と前記第１復号化手段により復号化された第１秘密鍵とを一方向性関数に入力して変換する関数変換手段と、

前記取得手段により取得された暗号化デジタル著作物を前記関数変換手段で得られた関数値で復号化する第２復号化手段とを備えることを特徴とする復号化装置。

【請求項３３】　記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、

暗号化されたデジタル著作物、その暗号化に用いられた媒体識別情報、前記媒体識別情報の暗号化に用いられた第１秘密鍵を暗号化した暗号化第１秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、

当該復号化装置に固有の第２秘密鍵を記憶する第２秘密鍵記憶手段と、

前記取得手段により取得された暗号化第１秘密鍵を前記第２秘密鍵記憶手段に記憶された第２秘密鍵で復号化する第１復号化手段と、

取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値

算出手段と、
前記第１復号化手段で復号化された第１秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、
前記取得手段により取得された媒体識別情報と前記変形手段で変形された属性値とを一方向性関数に入力して変換する関数変換手段と、
前記取得手段により取得された暗号化デジタル著作物を前記関数変換手段で得られた関数値で復号化する第２復号化手段とを備えることを特徴とする復号化装置。
【請求項３４】　記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、
暗号化されたデジタル著作物、その暗号化に用いられた媒体識別情報、前記媒体識別情報の暗号化に用いられた第１秘密鍵を暗号化した暗号化第１秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、
当該復号化装置に固有の第２秘密鍵を記憶する第２秘密鍵記憶手段と、
前記取得手段により取得された暗号化第１秘密鍵を前記第２秘密鍵記憶手段に記憶された第２秘密鍵で復号化する第１復号化手段と、
前記取得手段により取得された媒体識別情報と前記第１復号化手段で復号された第１秘密鍵とを一方向性関数に入力して変換する関数変換手段と、
取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記関数変換手段で得られた関数値を前記属性値算出手段により算出された属性値で変形させる変形手段と、
前記取得手段により取得された暗号化デジタル著作物を前記変形手段で変形された関数値で復号化する第２復号化手段とを備えることを特徴とする復号化装置。
【請求項３５】　暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、
デジタル著作物の暗号化に用いられた第１秘密鍵を暗号化した暗号化第１秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、
当該秘密鍵生成装置に固有の第２秘密鍵を記憶する第２秘密鍵記憶手段と、
取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記第２秘密鍵記憶手段に記憶された第２秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記取得手段により取得された暗号化第１秘密鍵を前記変形手段により変形された第２秘密鍵で復号化する第１復号化手段と、
前記第１復号化手段により復号化された第１秘密鍵を前記デジタル著作物の復号化のための秘密鍵として前記復号化装置に出力する出力手段とを備えることを特徴とする秘密鍵生成装置。
【請求項３６】　前記秘密鍵生成装置は、さらに、
前記第１復号化手段により復号化された第１秘密鍵が前記デジタル著作物の暗号化に用いられた正しい第１秘密鍵である否かを判定する判定手段を備えることを特徴とする請求項３５記載の秘密鍵生成装置。
【請求項３７】　前記判定手段は、
前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、
取得された確認データを前記第１復号化手段により復号化された第１秘密鍵で復号化する確認データ復号化部と、
前記確認データ復号化部による復号化によって得られたデータが所定の固定パターンに一致するか否かを判定し、一致する場合に、前記第１秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項３６記載の秘密鍵生成装置。
【請求項３８】　前記判定手段は、
前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、
前記第１復号化手段により復号化された第１秘密鍵を当該第１秘密鍵で暗号化する第１秘密鍵暗号化部と、
前記第１秘密鍵暗号化部により暗号化された第１秘密鍵が前記確認データ取得部により取得された確認データと一致するか否かを判定し、一致する場合に、前記第１秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項３６記載の秘密鍵生成装置。
【請求項３９】　前記判定手段は、
前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、
前記確認データ取得部により取得された確認データを前記第１復号化手段により復号化された第１秘密鍵で復号化する確認データ復号化部と、
前記確認データ復号化部により復号化された値と前記第１復号化手段により復号化された第１秘密鍵とが一致するか否かを判定し、一致する場合に、前記第１秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項３６記載の秘密鍵生成装置。
【請求項４０】　前記属性値算出手段は、前記公開鍵無効化リストのハッシュ値を前記属性値として算出し、
前記変形手段は、前記第２秘密鍵と前記ハッシュ値との排他的論理和をとることによって、前記第２秘密鍵を変形させることを特徴とする請求項３５記載の秘密鍵生成装置。

15

【請求項４１】　暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、
デジタル著作物の暗号化に用いられた第１秘密鍵を暗号化した暗号化第１秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、
当該復号化装置に固有の第２秘密鍵を記憶する第２秘密鍵記憶手段と、
前記取得手段により取得された暗号化第１秘密鍵を前記第２秘密鍵記憶手段に記憶された第２秘密鍵で復号化する第１復号化手段と、
前記取得手段に取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記第１復号化手段により復号化された第１秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、
前記変形手段で変形された第１秘密鍵を前記デジタル著作物の復号化のための秘密鍵として出力する出力手段とを備えることを特徴とする秘密鍵生成装置。
【請求項４２】　前記秘密鍵生成装置は、さらに、
前記変形手段により変形された第１秘密鍵が前記デジタル著作物の暗号化に用いられた正しい第１秘密鍵である否かを判定する判定手段を備えることを特徴とする請求項４１記載の秘密鍵生成装置。
【請求項４３】　前記判定手段は、
前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、
取得された確認データを前記変形手段で変形された第１秘密鍵で復号化する確認データ復号化部と、
前記確認データ復号化部による復号化によって得られたデータが所定の固定パターンに一致するか否かを判定し、一致する場合に、前記第１秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項４２記載の秘密鍵生成装置。
【請求項４４】　前記判定手段は、
前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、
前記変形手段により変形された第１秘密鍵を当該第１秘密鍵で暗号化する第１秘密鍵暗号化部と、
前記第１秘密鍵暗号化部により暗号化された第１秘密鍵が前記確認データ取得部により取得された確認データと一致するか否かを判定し、一致する場合に、前記第１秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項４２記載の秘密鍵生成装置。
【請求項４５】　前記判定手段は、
前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、
前記確認データ取得部により取得された確認データを前記変形手段により変形された第１秘密鍵で復号化する確認データ復号化部と、
前記確認データ復号化部により復号化された値と前記変形手段により変形された第１秘密鍵とが一致するか否かを判定し、一致する場合に、前記第１秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項４２記載の秘密鍵生成装置。

16

【請求項４６】　暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、
デジタル著作物の暗号化に用いられた媒体識別情報および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、
当該復号化装置に固有の第１秘密鍵を記憶する第１秘密鍵記憶手段と、
取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、
前記取得手段により取得された媒体識別情報と前記変形手段により変形された第１秘密鍵とを一方向性関数に入力して変換する関数変換手段と、
前記関数変換手段で得られた関数値を前記デジタル著作物の復号化のための秘密鍵として前記復号化装置に出力する出力手段とを備えることを特徴とする秘密鍵生成装置。
【請求項４７】　暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、
デジタル著作物の暗号化に用いられた媒体識別情報および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、
当該復号化装置に固有の第１秘密鍵を記憶する第１秘密鍵記憶手段と、
前記取得手段により取得された媒体識別情報と前記第１秘密鍵記憶手段に記憶された第１秘密鍵とを一方向性関数に入力して変換する関数変換手段と、
取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記関数変換手段で得られた関数値を前記属性値算出手段により算出された属性値で変形させる変形手段と、
前記変形手段で変形された属性値を前記デジタル著作物の復号化のための秘密鍵として出力する出力手段とを備えることを特徴とする秘密鍵生成装置。
【請求項４８】　暗号化されたデジタル著作物を復号化

する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、
デジタル著作物の暗号化に用いられた第１秘密鍵を暗号化した暗号化第１秘密鍵、前記第１秘密鍵の暗号化に用いられた第２秘密鍵を暗号化した暗号化第２秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、
当該秘密鍵生成装置に固有の第３秘密鍵を記憶する第３秘密鍵記憶手段と、
取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記第３秘密鍵記憶手段に記憶された第３秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、
前記取得手段により取得された暗号化第２秘密鍵を前記変形手段により変形された第３秘密鍵で復号化する第１復号化手段と、
前記取得手段により取得された暗号化第１秘密鍵を前記第１復号化手段により復号化された第２秘密鍵で復号化する第２復号化手段と、
前記第２復号化手段により復号化された第１秘密鍵を前記デジタル著作物の復号化のための秘密鍵として前記復号化装置に出力する出力手段とを備えることを特徴とする秘密鍵生成装置。
【請求項４９】　前記秘密鍵生成装置は、さらに、
前記第１復号化手段により復号化された第２秘密鍵が前記第１秘密鍵の暗号化に用いられた正しい第２秘密鍵である否かを判定する判定手段を備えることを特徴とする請求項４８記載の秘密鍵生成装置。
【請求項５０】　前記判定手段は、
前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、
取得された確認データを前記第１復号化手段により復号化された第２秘密鍵で復号化する確認データ復号化部と、
前記確認データ復号化部による復号化によって得られたデータが所定の固定パターンに一致するか否かを判定し、一致する場合に、前記第２秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項４９記載の秘密鍵生成装置。
【請求項５１】　前記判定手段は、
前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、
前記第１復号化手段により復号化された第２秘密鍵を当該第２秘密鍵で暗号化する第２秘密鍵暗号化部と、
前記第２秘密鍵暗号化部により暗号化された第２秘密鍵が前記確認データ取得部により取得された確認データと一致するか否かを判定し、一致する場合に、前記第２秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項４９記載の秘密鍵生成装置。

【請求項５２】　前記判定手段は、
前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、
前記確認データ取得部により取得された確認データを前記第１復号化手段により復号化された第２秘密鍵で復号化する確認データ復号化部と、
前記確認データ復号化部により復号化された値と前記第１復号化手段により復号化された第２秘密鍵とが一致するか否かを判定し、一致する場合に、前記第２秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項４９記載の秘密鍵生成装置。
【請求項５３】　暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、
デジタル著作物の暗号化に用いられた第１秘密鍵を暗号化した暗号化第１秘密鍵、前記第１秘密鍵の暗号化に用いられた第２秘密鍵を暗号化した暗号化第２秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、
当該復号化装置に固有の第３秘密鍵を記憶する第３秘密鍵記憶手段と、
前記取得手段により取得された暗号化第２秘密鍵を前記第３秘密鍵記憶手段に記憶された第３秘密鍵で復号化する第１復号化手段と、
取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記第１復号化手段で復号された第２秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、
前記取得手段により取得された暗号化第１秘密鍵を前記変形手段により変形された第２秘密鍵で復号化する第２復号化手段と、
前記第２復号化手段により復号化された第１秘密鍵を前記デジタル著作物の復号化のための秘密鍵として前記復号化装置に出力する出力手段とを備えることを特徴とする秘密鍵生成装置。
【請求項５４】　暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、
デジタル著作物の暗号化に用いられた第１秘密鍵を暗号化した暗号化第１秘密鍵、前記第１秘密鍵の暗号化に用いられた第２秘密鍵を暗号化した暗号化第２秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、
前記取得手段により取得された暗号化第２秘密鍵を前記

第１秘密鍵記憶手段に記憶された第３秘密鍵で復号化する第１復号化手段と、
前記取得手段により取得された暗号化第１秘密鍵を前記第１復号化手段により復号化された第２秘密鍵で復号化する第２復号化手段と、
取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記第２復号化手段により復号化された第１秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、
前記第２復号化手段により復号化された第１秘密鍵を前記デジタル著作物の復号化のための秘密鍵として前記復号化装置に出力する出力手段とを備えることを特徴とする秘密鍵生成装置。

【請求項５５】　暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、
デジタル著作物の暗号化に用いられた媒体識別情報、前記媒体識別情報の暗号化に用いられた第１秘密鍵を暗号化した暗号化第１秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、
当該秘密鍵生成装置に固有の第２秘密鍵を記憶する第２秘密鍵記憶手段と、
取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記第２秘密鍵記憶手段に記憶された第２秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、
前記取得手段により取得された暗号化第１秘密鍵を前記変形手段により変形された第２秘密鍵で復号化する第１復号化手段と、
前記取得手段により取得された媒体識別情報と前記第１復号化手段により復号化された第１秘密鍵とを一方向性関数に入力して変換する関数変換手段と、
前記関数変換手段で得られた関数値を前記デジタル著作物の復号化のための秘密鍵として前記復号化装置に出力する出力手段とを備えることを特徴とする秘密鍵生成装置。

【請求項５６】　前記秘密鍵生成装置は、さらに、
前記第１復号化手段により復号化された第１秘密鍵が前記媒体識別情報の暗号化に用いられた正しい第１秘密鍵である否かを判定する判定手段を備えることを特徴とする請求項５５記載の秘密鍵生成装置。

【請求項５７】　前記判定手段は、
前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、
取得された確認データを前記第１復号化手段により復号化された第１秘密鍵で復号化する確認データ復号化部と、
前記確認データ復号化部による復号化によって得られたデータが所定の固定パターンに一致するか否かを判定し、一致する場合に、前記第１秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項５６記載の秘密鍵生成装置。

【請求項５８】　前記判定手段は、
前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、
前記第１復号化手段により復号化された第１秘密鍵を当該第１秘密鍵で暗号化する第１秘密鍵暗号化部と、
前記第１秘密鍵暗号化部により暗号化された第１秘密鍵が前記確認データ取得部により取得された確認データと一致するか否かを判定し、一致する場合に、前記第１秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項５６記載の秘密鍵生成装置。

【請求項５９】　前記判定手段は、
前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、
前記確認データ取得部により取得された確認データを前記第１復号化手段により復号化された第１秘密鍵で復号化する確認データ復号化部と、
前記確認データ復号化部により復号化された値と前記第１復号化手段により復号化された第１秘密鍵とが一致するか否かを判定し、一致する場合に、前記第１秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項５６記載の秘密鍵生成装置。

【請求項６０】　暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、
デジタル著作物の暗号化に用いられた媒体識別情報、前記媒体識別情報の暗号化に用いられた第１秘密鍵を暗号化した暗号化第１秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、
当該復号化装置に固有の第２秘密鍵を記憶する第２秘密鍵記憶手段と、
前記取得手段により取得された暗号化第１秘密鍵を前記第２秘密鍵記憶手段に記憶された第２秘密鍵で復号化する第１復号化手段と、
取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、
前記第１復号化手段で復号化された第１秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、
前記取得手段により取得された媒体識別情報と前記変形手段で変形された属性値とを一方向性関数に入力して変換する関数変換手段と、

前記関数変換手段で得られた関数値を前記デジタル著作物の復号化のための秘密鍵として前記復号化装置に出力する出力手段とを備えることを特徴とする秘密鍵生成装置。

【請求項６１】　暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、

デジタル著作物の暗号化に用いられた媒体識別情報、前記媒体識別情報の暗号化に用いられた第１秘密鍵を暗号化した暗号化第１秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、

当該復号化装置に固有の第２秘密鍵を記憶する第２秘密鍵記憶手段と、

前記取得手段により取得された暗号化第１秘密鍵を前記第２秘密鍵記憶手段に記憶された第２秘密鍵で復号化する第１復号化手段と、

前記取得手段により取得された媒体識別情報と前記第１復号化手段で復号された第１秘密鍵とを一方向性関数に入力して変換する関数変換手段と、

取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記関数変換手段で得られた関数値を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記変形手段で変形された関数値を前記デジタル著作物の復号化のための秘密鍵として前記復号化装置に出力する出力手段とを備えることを特徴とする秘密鍵生成装置。

【請求項６２】　記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項１記載の暗号化装置と請求項２４記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項６３】　記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項５記載の暗号化装置と請求項２５記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項６４】　記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項６記載の暗号化装置と請求項２６記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項６５】　記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項１０記載の暗号化装置と請求項２７記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項６６】　記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項１１記載の暗号化装置と請求項２８記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項６７】　記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項１２記載の暗号化装置と請求項２９記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項６８】　記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項１６記載の暗号化装置と請求項３０記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項６９】　記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項１７記載の暗号化装置と請求項３１記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項７０】　記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項１８記載の暗号化装置と請求項３２記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項７１】　記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項２２記載の暗号化装置と請求項３３記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項７２】　記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項２３記載の暗号化装置と請求項３４記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項７３】　相手装置の公開鍵を用いて相手装置と暗号通信する装置であって、

無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する記憶手段と、

新たな公開鍵無効化リストを取得する取得手段と、

取得された公開鍵無効化リストのサイズと前記記憶手段に記憶されている公開鍵無効化リストのサイズとを比較し、取得された公開鍵無効化リストのサイズが大きい場合に、取得された公開鍵無効化リストを前記記憶手段に格納して更新する格納手段と、

前記記憶手段に格納された公開鍵無効化リストを参照して相手装置の公開鍵の有効性を判断し、有効と判断した場合に、その公開鍵を用いて相手装置と暗号通信する通信手段とを備えることを特徴とする暗号通信装置。

【請求項７４】　相手装置の公開鍵を用いて相手装置と暗号通信する装置であって、

無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する記憶手段と、

新たな公開鍵無効化リストを取得する取得手段と、

取得された公開鍵無効化リストに示された前記証明書の数と前記記憶手段に記憶されている公開鍵無効化リストに示された前記証明書の数とを比較し、取得された公開鍵無効化リストに示された前記証明書の数が大きい場合に、取得された公開鍵無効化リストを前記記憶手段に格納して更新する格納手段と、

前記記憶手段に格納された公開鍵無効化リストを参照して相手装置の公開鍵の有効性を判断し、有効と判断した場合に、その公開鍵を用いて相手装置と暗号通信する通信手段とを備えることを特徴とする暗号通信装置。

【請求項７５】　デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置において、ｎ（≧２）個の秘密鍵のうち、第１秘密鍵を用いてデジタル著作物を暗号化するとともに、第ｉ（２≦ｉ≦ｎ）秘密鍵を用いて第（ｉ－１）秘密鍵を暗号化するという暗号化の連鎖を前記第１～第（ｎ－１）秘密鍵について繰り返し、暗号化された第１～第（ｎ－１）秘密鍵を前記媒体に出力する方法であって、

前記第１～第ｎ秘密鍵の少なくとも１つを用いた暗号化においては、その暗号化に先立ち、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストの内容に依存する属性値を用いて秘密鍵を変形させておく第１ステップを含むことを特徴とする暗号化方法。

【請求項７６】　デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置において、ｎ（≧１）個の秘密鍵のうち、第１秘密鍵を用いて媒体識別情報を一方向性関数で変換した後に、変換された媒体識別情報でデジタル著作物を暗号化するとともに、前記ｎが２以上の場合に、第ｉ（２≦ｉ≦ｎ）秘密鍵を用いて第（ｉ－１）秘密鍵を暗号化するという暗号化の連鎖を前記第１～第（ｎ－１）秘密鍵について繰り返し、暗号化された第１～第（ｎ－１）秘密鍵を前記媒体に出力する方法であって、

前記第１～第ｎ秘密鍵の少なくとも１つを用いた暗号化又は変換においては、（ｉ）その暗号化又は変換に先立ち、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストの内容に依存する属性値を用いて秘密鍵を変形させておくか、又は、（２）前記変換によって得られた媒体識別情報を前記属性値で変形させておく第２ステップを含むことを特徴とする暗号化方法。

【請求項７７】　暗号化されたデジタル著作物を復号化する復号化装置において、暗号化されたデジタル著作物とｎ（≧２）個の暗号化秘密鍵と無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストとを記録媒体又は伝送媒体を介して取得した後に、予め保持している秘密鍵を用いて前記ｎ個の暗号化秘密鍵のうちの第１暗号化秘密鍵を復号化し、得られた第１秘密鍵で第２暗号化秘密鍵を復号化するという復号化の連鎖を前記ｎ個の暗号化秘密鍵について繰り返し、最後の復号化で得られた第ｎ秘密鍵でデジタル著作物を復号化する方法であって、

前記第１～第ｎ暗号化秘密鍵に対する復号化の少なくとも１つおいては、その復号化に先立ち、復号化に用いる秘密鍵を前記公開鍵無効化リストの内容に依存する属性値で変形させておく第３ステップを含むことを特徴とする復号化方法。

【請求項７８】　暗号化されたデジタル著作物を復号化する復号化装置において、暗号化されたデジタル著作物と媒体識別情報とｎ（≧１）個の暗号化秘密鍵と無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストとを記録媒体又は伝送媒体を介して取得した後に、予め保持している秘密鍵を用いて前記ｎ個の暗号化秘密鍵のうちの第１暗号化秘密鍵を復号化し、前記ｎが２以上の場合に、前記復号化で得られた第１秘密鍵で第２暗号化秘密鍵を復号化するという復号化の連鎖を前記ｎ個の暗号化秘密鍵について繰り返し、最後の復号化で得られた第ｎ秘密鍵を用いて前記媒体識別情報を一方向性関数で変換し、変換後の媒体識別情報でデジタル著作物を復号化する方法であって、

前記第１～第ｎ暗号化秘密鍵に対する復号化及び前記媒体識別情報に対する変換の少なくとも１つおいては、

（１）その復号化又は変換に先立ち、復号化又は変換に用いる秘密鍵を前記公開鍵無効化リストの内容に依存する属性値で変形させておくか、又は、（２）前記変換によって得られた媒体識別情報を前記属性値で変形させておく第４ステップを含むことを特徴とする復号化方法。

【請求項７９】　暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置において、ｎ（≧２）個の暗号化秘密鍵と無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得した後に、予め保持している秘密鍵を用いて前記ｎ個の暗号化秘密鍵のうちの第１暗号化秘密鍵を復号化し、得られた第１秘密鍵で第２暗号化秘密鍵を復号化するという復号化の連鎖を前記ｎ個の暗号化秘密鍵について繰り返し、最後の復号化で得られた第ｎ秘密鍵を前

記復号化装置に出力する方法であって、
前記第１～第ｎ暗号化秘密鍵に対する復号化の少なくとも１つおいては、その復号化に先立ち、復号化に用いる秘密鍵を前記公開鍵無効化リストの内容に依存する属性値で変形させておく第５ステップを含むことを特徴とする秘密鍵生成方法。

【請求項８０】　暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置において、媒体識別情報とｎ（≧１）個の暗号化秘密鍵と無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストとを記録媒体又は伝送媒体を介して取得した後に、予め保持している秘密鍵を用いて前記ｎ個の暗号化秘密鍵のうちの第１暗号化秘密鍵を復号化し、前記ｎが２以上の場合に、前記復号化で得られた第１秘密鍵で第２暗号化秘密鍵を復号化するという復号化の連鎖を前記ｎ個の暗号化秘密鍵について繰り返し、最後の復号化で得られた第ｎ秘密鍵を用いて前記媒体識別情報を一方向性関数で変換し、変換後の媒体識別情報を前記復号化装置に出力する方法であって、
前記第１～第ｎ暗号化秘密鍵に対する復号化及び前記媒体識別情報に対する変換の少なくとも１つおいては、
（１）その復号化又は変換に先立ち、復号化又は変換に用いる秘密鍵を前記公開鍵無効化リストの内容に依存する属性値で変形させておくか、又は、（２）前記変換によって得られた媒体識別情報を前記属性値で変形させておく第６ステップを含むことを特徴とする秘密鍵生成方法。

【請求項８１】　デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置に用いられるプログラムであって、
請求項７５又は７６記載の暗号化方法におけるステップをコンピュータに実行させることを特徴とするプログラム。

【請求項８２】　記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置に用いられるプログラムであって、
請求項７７又は７８記載の復号化方法におけるステップをコンピュータに実行させることを特徴とするプログラム。

【請求項８３】　暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置に用いられるプログラムであって、
請求項７９又は８０記載の秘密鍵生成方法におけるステップをコンピュータに実行させることを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、記録媒体又は伝送媒体を介してデジタル著作物を転送する際の著作権保護

を図る暗号化装置および復号化装置等に関し、特に、無効化された公開鍵証明書を特定する公開鍵証明書無効化リストの差し替え攻撃に対する防御技術に関する。

【０００２】

【従来の技術】デジタル著作物を第１の機器から第２の機器に転送する際に、不正取得による著作権侵害を防止するために、転送に先立ち、第１の機器が第２の機器を認証する（あるいは、相互に認証する）ことが行われる。つまり、通信相手が確かに自分が意図している相手かどうかを確認することが行われる。

【０００３】例えば、公開鍵暗号を用いた例として、第１の機器が第２の機器に乱数を送信し、続いて、第２の機器がその乱数に対して自分の秘密鍵で暗号化（電子署名など）して第１の機器に返信し、最後に、返信されてきた暗号文（あるいは、署名文）に対して、第１の機器が第２の機器の公開鍵を用いて検証するというものである。ところが、このような公開鍵暗号を用いた認証においては、公開鍵そのものが有効なものであることが前提となる。

【０００４】そこで、最近では、認証局と呼ばれる機関あるいは企業から、各ユーザに対応する正しい公開鍵であることを示す（公開鍵に対する「お墨付き」となる）「公開鍵証明書」が発行されるようになってきた。そして、発行された公開鍵証明書のうち、有効期限の過ぎたものや、不正を働いたユーザあるいは秘密鍵が盗まれたユーザの公開鍵証明書等については、それらを無効化させるために（無効化していることを他のユーザに知らせるために）、無効化した公開鍵証明書を特定する情報の一覧を示す公開鍵証明書無効化リスト（Certificate Revocation List；以下、「ＣＲＬ」、「公開鍵無効化リスト」又は「無効化リスト」等とも記す。）が発行されている。

【０００５】したがって、通信相手の公開鍵を用いてその通信相手を認証する際には、その通信相手から公開鍵証明書を入手し、入手した公開鍵証明書が公開鍵証明書無効化リストに登録されたもの（無効化されたもの）でないことを確認した上で、上述の認証処理を行うことで、不正な通信相手に貴重なデジタル著作物を渡してしまうことを回避することができる。

【０００６】なお、公開鍵証明書だけを用いて鍵を検証しているものもあるが（例えば、特許文献１参照。）、上記したように、有効期限の過ぎたものや、不正を働いたユーザあるいは秘密鍵が盗まれたユーザの公開鍵証明書等については、対処できない。

【０００７】

【特許文献１】特許第３１９９１１９号公報（第２頁）

【０００８】

【発明が解決しようとする課題】しかしながら、あらゆる機器が、正規の公開鍵証明書無効化リストを入手して通信相手の公開鍵証明書の有効性をチェックできるとは

限らず、そのために、その弱点を利用した不正行為が行われる可能性がある。

【０００９】例えば、映画等のデジタル著作物が記録されたＤＶＤ（Digital Video/Versatile Disc）を再生するＤＶＤドライブ装置等の機器が、ＤＶＤを介して正規の公開鍵証明書無効化リストを取得し（ＤＶＤに記録された最新の公開鍵証明書無効化リストを読み出し）、その公開鍵証明書無効化リストを用いて、相手機器（内蔵の再生処理回路や再生用ソフトウェアが稼動するコンピュータ等）を認証する方法を採用した場合には、公開鍵証明書無効化リストを読み出す過程において、例えば、古い公開鍵証明書無効化リストに差し替えられてしまう可能性がある。そのために、正規の（例えば、最新の）公開鍵証明書無効化リストであれば無効化された公開鍵証明書として登録されているにも拘わらず、すり替えられた古い公開鍵証明書無効化リストには未だ登録されていない無効な公開鍵を用いて、不正にデジタル著作物が取得されてしまうという攻撃を受け得る。

【００１０】また、既に公開鍵証明書無効化リストを保持している機器が新たな公開鍵証明書無効化リストを入手した際に、いずれの公開鍵証明書無効化リストがより最新であるか、すなわち、保存しておくべき公開鍵証明書無効化リストはいずれであるかを的確に判断する必要もある。

【００１１】そこで、本発明は、このような状況に鑑みてなされたものであり、公開鍵証明書無効化リストの差し替えという攻撃に対して防御することができ、安全にデジタル著作物を転送することを可能にする暗号化装置、復号化装置、秘密鍵生成装置、著作権保護システムおよび暗号通信装置を提供することを第１の目的とする。また、本発明の第２の目的は、公開鍵証明書無効化リストを用いて暗号通信をする装置において、新たな公開鍵証明書無効化リストを入手したときに、より最新のものを的確に特定し、古いものに代えて、より最新の公開鍵証明書無効化リストを保持することを可能にすることである。

【００１２】

【課題を解決するための手段】上記第１の目的を達成するために、本発明に係る暗号化装置は、デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、デジタル著作物を記憶するデジタル著作物記憶手段と、デジタル著作物の暗号化に用いられる第１秘密鍵を記憶する第１秘密鍵記憶手段と、暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第２秘密鍵を記憶する第２秘密鍵記憶手段と、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第２秘密鍵記憶手段に記憶された第２秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記変形手段により変形された第２秘密鍵で暗号化する第１暗号化手段と、前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記第１秘密鍵記憶手段に記憶された第１秘密鍵で暗号化する第２暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第１暗号化手段により暗号化された第１秘密鍵および前記第２暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする。

【００１３】ここで、前記暗号化装置は、さらに、前記復号化装置のおいて復号化された第１秘密鍵が正しいものであるか否かを確認するための基準となる確認データを前記記録媒体又は伝送媒体に出力する確認データ出力手段を備えてもよい。例えば、前記確認データ出力手段は、所定の固定パターンのデータを前記第１秘密鍵記憶手段に記憶された第１秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力したり、前記確認データ出力手段は、前記第１秘密鍵記憶手段に記憶された第１秘密鍵を当該第１秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力してもよい。

【００１４】また、本発明に係る暗号化装置は、デジタル著作物であるデジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、デジタル著作物を記憶するデジタル著作物記憶手段と、デジタル著作物の暗号化に用いられる第１秘密鍵を記憶する第１秘密鍵記憶手段と、暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第２秘密鍵を記憶する第２秘密鍵記憶手段と、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記第２秘密鍵記憶手段に記憶された第２秘密鍵で暗号化する第１暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記変形手段により変形された第１秘密鍵で暗号化する第２暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第１暗号化手段により暗号化された第１秘密鍵および前記第２暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする。

【００１５】また、上記第２の目的を達成するために、

本発明に係る暗号通信装置は、相手装置の公開鍵を用いて相手装置と暗号通信する装置であって、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する記憶手段と、新たな公開鍵無効化リストを取得する取得手段と、取得された公開鍵無効化リストのサイズと前記記憶手段に記憶されている公開鍵無効化リストのサイズとを比較し、取得された公開鍵無効化リストのサイズが大きい場合に、取得された公開鍵無効化リストを前記記憶手段に格納して更新する格納手段と、前記記憶手段に格納された公開鍵無効化リストを参照して相手装置の公開鍵の有効性を判断し、有効と判断した場合に、その公開鍵を用いて相手装置と暗号通信する通信手段とを備えることを特徴とする。同様に、上記格納手段に代えて、取得された公開鍵無効化リストに示された前記証明書の数と前記記憶手段に記憶されている公開鍵無効化リストに示された前記証明書の数とを比較し、取得された公開鍵無効化リストに示された前記証明書の数が大きい場合に、取得された公開鍵無効化リストを前記記憶手段に格納して更新する格納手段とすることもできる。

【００１６】なお、本発明は、上記暗号化装置に対応する復号化装置あるいは秘密鍵生成装置として実現したり、それら暗号化装置および復号化装置からなる著作権保護システムとして実現したり、それら暗号化装置、復号化装置および暗号通信装置を構成する特徴的な手段をステップとする暗号化方法、復号化方法および暗号通信方法として実現したり、それらステップをパーソナルコンピュータ等に実行させるプログラムとして実現したりすることもできる。そして、そのプログラムをＤＶＤ等の記録媒体やインターネット等の伝送媒体を介して広く流通させることができるのは言うまでもない。

【００１７】

【発明の実施の形態】以下、本発明の実施の形態に係る著作権保護システムについて、図面を用いて詳細に説明する。

【００１８】（実施の形態１）図１は、本実施の形態１に係る記録メディア用著作権保護システムの全体構成を示す機能ブロック図である。記録メディア用著作権保護システム１ａは、記録メディアとしてのＤＶＤ２ａに暗号化されたコンテンツ等を記録したり、ＤＶＤ２ａから暗号化されたコンテンツ等を読み出してコンテンツを復号化したりするものであり、ＤＶＤ２ａに暗号化されたコンテンツ等を記録する暗号化装置１００ａと、ＤＶＤ２ａから暗号化されたコンテンツ等を読み出してコンテンツを復号化する復号化装置２００ａと、公開鍵証明書無効化リストＣＲＬ等を発行する公開鍵証明書認証局（Certificate Authority）ＣＡが使用する端末装置３００などから構成される。

【００１９】暗号化装置１００ａは、大きく分けて、２台の端末装置、すなわち、著作権保護ライセンサが使用

する端末装置１１０ａと、コンテンツ製造メーカが使用する端末装置１６０とから構成される。

【００２０】復号化装置２００ａは、例えば画質レベルＨＤ（１１２５ｉ／７５０ｐ）でのコンテンツ再生に対応したＨＤ－ＤＶＤプレーヤ等であって、著作権保護ライセンサが供給するＩＣカード２１０ａと、このプレーヤの製造メーカのデスクランブラ２６０と、ＤＶＤ２ａから暗号化されたコンテンツ等を読み出すＤＶＤ－ＲＯＭドライブ（不図示）等とからなる。

【００２１】著作権保護ライセンサが使用する端末装置１１０ａは、復号化装置２００ａにおいて著作権保護を図るための情報、すなわち公開鍵証明書無効化リストＣＲＬ、コンテンツを復号化するためのコンテンツ鍵、このコンテンツ鍵を暗号化した暗号化コンテンツ鍵の束を端末装置１６０に提供するコンピュータ装置であり、その機能として、公開鍵無効化リスト記憶部１１１と、デバイス鍵束記憶部１１２と、コンテンツ鍵記憶部１１３と、ハッシュ関数処理部１１４と、Ｅｘ－ＯＲ部１１５と、Ｅｎｃ部１１６等とを備える。

【００２２】公開鍵無効化リスト記憶部１１１は、インターネット等の通信網を介して端末装置３００に定期的にアクセスし、公開鍵証明書認証局ＣＡが提供する最新の公開鍵証明書無効化リストＣＲＬを定期的に更新記憶する。この公開鍵証明書無効化リストＣＲＬは、図２に示されるように、ファイルヘッダと、「全般」のフィールドと、「無効リスト」のフィールド等とからなる。ファイルヘッダには、ファイルの「名前」○△□△．ｃｒｌ、ファイルの「サイズ」７９ＫＢ、ファイルの「種類」証明書無効リスト、ファイルの「更新日」２００１／０９／０７／１２：３４のレコードを含む。また、「全般」フィールドには、「バージョン」Ｖ１、「発行者」○△□△、「有効開始日」２００１年９月６日、「次の更新予定日」２００１年９月１６日、「署名アルゴリズム」ｍｄ５ＲＡＳのレコードを含む。また、「無効リスト」のフィールドには、無効となった証明書のシリアル番号と、その無効日とのレコードがテキスト形式で記載されている。この公開鍵証明書無効化リストＣＲＬは、時が経つにつれて無効となった証明書の数が単調の増え続けるため、最新版であるほど、無効となった証明書のシリアル番号のエントリー数（リスト登録台数）が単調増加し、ファイルの「サイズ」が単調的に大きくなる性質を有している。

【００２３】デバイス鍵束記憶部１１２は、著作権保護ライセンサが供給するＩＣカード２１０ａごとに固有のデバイス鍵ＫＤ＿Ａ（例えば、１２８ｂｉｔ）を束にして予め記憶する。

【００２４】コンテンツ鍵記憶部１１３は、映画や音楽等の所定のコンテンツを暗号化するための秘密鍵であるコンテンツ鍵Ｋｃ（例えば、１２８ｂｉｔ）を記憶する。

31

【００２５】ハッシュ関数処理部１１４は、ハッシュ関数にしたがって、公開鍵無効化リスト記憶部１１１に記憶された可変長のデータである公開鍵証明書無効化リストＣＲＬを圧縮して固定長（例えば、１２８ｂｉｔ）のデータ（ハッシュ値Ｈａｓｈ）に変換する処理部であり、例えば、ＳＨＡ－１（Secure Hash Algorithm-1）やＭＤ５などにしたがって変換する。

【００２６】Ｅｘ－ＯＲ部１１５は、ハッシュ関数処理部１１４により算出されたハッシュ値Ｈａｓｈと、デバイス鍵束記憶部１１２に記憶された各デバイス鍵ＫＤ＿Ａとの排他的論理和をとる（各デバイス鍵ＫＤ＿Ａをハッシュ値Ｈａｓｈで変形させる）。

【００２７】Ｅｎｃ部１１６は、コンテンツ鍵記憶部１１３に記憶されたコンテンツ鍵ＫｃをＥｘ－ＯＲ部１１５の出力、すなわちハッシュ値Ｈａｓｈと各デバイス鍵ＫＤ＿Ａとの排他的論理和値で暗号化し、暗号化コンテンツ鍵の束を生成する。

【００２８】なお、この端末装置１１０ａのハッシュ関数処理部１１４およびＥｘ－ＯＲ部１１５は、公開鍵無効化リスト記憶部１１１に記憶された公開鍵証明書無効化リストＣＲＬに依存させてデバイス鍵ＫＤ＿Ａを変形させているが、これは、変形されたデバイス鍵ＫＤ＿Ａでコンテンツ鍵Ｋｃを暗号化させることで、Ｅｎｃ部１１６から出力される暗号化コンテンツ鍵と公開鍵証明書無効化リストＣＲＬとを関連付けるためである。これによって、後述する復号化装置２００ａでの復号処理において、公開鍵証明書無効化リストＣＲＬの差し替えという攻撃に対して防御することが可能となる。

【００２９】コンテンツ製造メーカが使用する端末装置１６０は、端末装置１１０ａから渡された公開鍵証明書無効化リストＣＲＬや、暗号化コンテンツ鍵の束をそのままＤＶＤ２ａに記録したりする書き込み装置であり、その機能として、コンテンツ記憶部１６１と、Ｅｎｃ部１６２等とを備える。

【００３０】コンテンツ記憶部１６１は、映画や音楽等の所定のコンテンツを予め記憶する。

【００３１】Ｅｎｃ部１６２は、コンテンツ記憶部１６１に記憶されたコンテンツを、端末装置１１０ａから渡されたコンテンツ鍵Ｋｃで暗号化し、暗号化コンテンツを生成する。

【００３２】このように２台の端末装置１１０ａ、１６０から構成された暗号化装置１００ａにおいては、ＤＶＤ２ａを製造する場合、端末装置１１０ａは、公開鍵無効化リスト記憶部１１１から公開鍵無効化リストＣＲＬを読み出して、読み出した公開鍵無効化リストＣＲＬをハッシュ関数処理部１１４と、端末装置１６０とに渡す。ハッシュ関数処理部１１４は、公開鍵無効化リストＣＲＬのハッシュ値Ｈａｓｈを計算し、計算したハッシュ値ＨａｓｈをＥｘ－ＯＲ部１１５に渡す。Ｅｘ－ＯＲ部１１５は、デバイス鍵束記憶部１１２からデバイス鍵

32

ＫＤ＿Ａ、…を１つずつ読み出し、読み出すごとにデバイス鍵ＫＤ＿Ａ、…とハッシュ値Ｈａｓｈとの排他的論理和を順次計算し、各排他的論理和値をＥｎｃ部１１６に出力する。そして、端末装置１１０ａは、コンテンツ鍵記憶部１１３からコンテンツ鍵Ｋｃを読み出して、読み出したコンテンツ鍵ＫｃをＥｎｃ部１１６と、端末装置１６０とに渡す。Ｅｎｃ部１１６は、渡されたコンテンツ鍵ＫｃをＥｘ－ＯＲ部１１５から出力された各排他的論理和値で暗号化する。すなわち、Ｅｎｃ部１１６は、デバイス鍵ＫＤ＿Ａのそれぞれの値とハッシュ値Ｈａｓｈとの排他的論理和値を鍵として、コンテンツ鍵Ｋｃを暗号化する。これにより、Ｅｎｃ部１１６は、暗号化したコンテンツ鍵を複数生成し、暗号化コンテンツ鍵を束にして端末装置１６０に渡す。

【００３３】端末装置１６０は、端末装置１１０ａから渡された公開鍵無効化リストＣＲＬと、暗号化コンテンツ鍵の束とを、そのままＤＶＤ２ａに書き込む。そして、Ｅｎｃ部１６２により生成された暗号化コンテンツをＤＶＤ２ａに書き込む。このようにして製造されたＤＶＤ２ａは、暗号化コンテンツと共に、暗号化コンテンツ鍵の束と、製造時点で最新の公開鍵無効化リストＣＲＬとがバインドされた状態でユーザに販売される。

【００３４】一方、このようなＤＶＤ２ａを復号化する復号化装置２００ａのＩＣカード２１０ａは、コンピュータのプログラムを故意の変更から防ぐために使用されるモジュール（TRM:Tamper Resistance Module）で構成され、公開鍵証明書無効化リストＣＲＬに載るような不正なデスクランブラ２６０を排除することにより著作権を保護するものであって、大きく分けて、ＤＶＤ２ａにバインドされた公開鍵証明書無効化リストＣＲＬに基づいて暗号化コンテンツを復号するための鍵を取得するコンテンツ鍵復号部２２０ａと、公開鍵無効化リストＣＲＬにより通信相手（デスクランブラ２６０）がＲｅｖｏｋｅ（無効化）されていないかどうかをチェックしつつ、デスクランブラ２６０との間の相互認証形式でＳＡＣ（SecureAuthentication Channel：認証付け安全な通信路）を設定するための認証処理部２３０ａとを備える。

【００３５】認証処理部２３０ａは、証明書認証局用公開鍵記憶部２３１と、ＩＣカード用秘密鍵記憶部２３２と、ＩＣカード用（著作権保護ライセンサ用）公開鍵証明書記憶部２３３と、乱数生成部２３４と、公開鍵無効化リストチェック部２３５と、楕円曲線暗号処理部２３６と、認証部２３７と、バッファメモリ２３８等とからなる。

【００３６】証明書認証局用公開鍵記憶部２３１は、公開鍵証明書認証局ＣＡの署名を解読するのに用いる認証局用公開鍵ＰＫ＿ＣＡを予め記憶する。

【００３７】ＩＣカード用秘密鍵記憶部２３２は、著作権保護ライセンサから供給されたＩＣカード２１０ａが

自己の署名に用いるＩＣカードに固有のＩＣカード用秘密鍵ＳＫ＿Ａを予め記憶する。

【００３８】ＩＣカード用公開鍵証明書記憶部２３３は、公開鍵ＰＫ＿ＡがＩＣカード２１０ａのものであることを公開鍵証明書認証局ＣＡが証明する書類であるＩＣカード用公開鍵証明書Ｃｅｒｔ＿Ａを予め記憶する。このＩＣカード用公開鍵証明書Ｃｅｒｔ＿Ａは、図３に示されるように、ＩＣカード２１０ａ（著作権保護ライセンサ）のＩＤや、ＩＣカード用秘密鍵ＳＫ＿Ａに対するＩＣカード用公開鍵ＰＫ＿Ａ、ＩＣカード用公開鍵ＰＫ＿Ａに対する証明書認証局ＣＡの署名、（証明書の）有効期限等から構成される。

【００３９】乱数生成部２３４は、時変の値として乱数（例えば、１２８ｂｉｔ）を生成する。

【００４０】公開鍵無効化リストチェック部２３５は、公開鍵無効化リストＣＲＬに相手（デスクランブラ２６０）のＩＤが含まれているか否かをチェックする。

【００４１】楕円曲線暗号処理部２３６は、ＳＡＣ設定における認証等の際に、楕円曲線にしたがった暗号処理（例えば、２５６ｂｉｔの処理単位）を実行する。

【００４２】認証部２３７は、ＳＡＣを介してデスクランブラ２６０と通信する通信インタフェースである。

【００４３】バッファメモリ２３８は、乱数生成部２３４が生成した乱数や、楕円曲線暗号処理部２３６が生成した一時的なデータを保持する。

【００４４】コンテンツ鍵復号部２２０は、デバイス鍵記憶部２２１と、ハッシュ関数処理部２２２と、Ｅｘ－ＯＲ部２２３と、Ｄｅｃ処理部２２４とを備える。

【００４５】デバイス鍵記憶部２２１は、ＩＣカード２１０ａに固有のデバイス鍵ＫＤ＿Ａ（秘密鍵であり、例えば、ＡＥＳ１２８ｂｉｔの鍵）を記憶する。

【００４６】ハッシュ関数処理部２２２は、端末装置１１０ａのハッシュ関数処理部１１４と同様に構成され、ＤＶＤ２ａにバインドされた公開鍵証明書無効化リストＣＲＬのハッシュ値Ｈａｓｈ（例えば、１２８ｂｉｔ）を算出する。

【００４７】Ｅｘ－ＯＲ部２２３は、デバイス鍵記憶部２２１に記憶されたデバイス鍵ＫＤ＿Ａと、ハッシュ関数処理部２２２により算出されたハッシュ値Ｈａｓｈとの排他的論理和をとる（つまり、デバイス鍵ＫＤ＿Ａをハッシュ値Ｈａｓｈで変形させる）。

【００４８】Ｄｅｃ処理部２２４は、ＤＶＤ２ａにバインドされた暗号化コンテンツ鍵の束の中から予め定められた場所に記録されている自己用の暗号化コンテンツ鍵を、デバイス鍵ＫＤ＿Ａとハッシュ値Ｈａｓｈとの排他的論理和値で復号化し、コンテンツ鍵Ｋｃを生成する。

【００４９】デスクランブラ２６０は、ＩＣカード２１０ａと同様、コンピュータプログラムの不正な改ざんを防ぐために使用されるモジュールで構成され、大きく分けて、公開鍵無効化リストＣＲＬにより通信相手（ＩＣカード２１０ａ）がＲｅｖｏｋｅされていないかどうかをチェックしつつ、ＩＣカード２１０ａとの間の相互認証形式でＳＡＣを設定するための認証処理部２７０と、ＤＶＤ２ａから読み出した暗号化コンテンツを、ＩＣカード２１０ａから渡されたコンテンツ鍵Ｋｃで復号し、コンテンツを取得するＤｅｃ処理部２８０とを備える。

【００５０】認証処理部２７０は、証明書認証局用公開鍵記憶部２７１と、デスクランブラ用秘密鍵記憶部２７２と、デスクランブラ用（プレーヤメーカ用）公開鍵証明書記憶部２７３と、乱数生成部２７４と、公開鍵無効化リストチェック部２７５と、楕円曲線暗号処理部２７６と、認証部２７７と、バッファメモリ２７８等とからなる。

【００５１】証明書認証局用公開鍵記憶部２７１は、証明書認証局ＣＡの証明書認証局用公開鍵ＰＫ＿ＣＡを予め記憶する。

【００５２】デスクランブラ用秘密鍵記憶部２７２は、このＨＤ－ＤＶＤプレーヤ２００のメーカにより供給され、デスクランブラ２６０が自己の署名に用いるデスクランブラに固有のデスクランブラ用秘密鍵ＳＫ＿ｉを予め記憶する。

【００５３】デスクランブラ用公開鍵証明書記憶部２７３は、公開鍵ＰＫ＿ｉがプレーヤメーカのものであることを公開鍵証明書認証局ＣＡが証明する書類であるデスクランブラ用公開鍵証明書Ｃｅｒｔ＿ｉを予め記憶する。このデスクランブラ用公開鍵証明書Ｃｅｒｔ＿ｉは、図４に示されるように、デスクランブラ２６０（プレーヤメーカ）のＩＤ（証明書のシリアル番号）や、デスクランブラ用秘密鍵ＳＫ＿ｉに対するデスクランブラ用公開鍵ＰＫ＿ｉ、デスクランブラ用公開鍵ＰＫ＿ｉに対する証明書認証局ＣＡの署名、（証明書の）有効期限等から構成される。

【００５４】乱数生成部２７４は、時変の値として乱数（例えば、１２８ｂｉｔ）を生成する。

【００５５】公開鍵無効化リストチェック部２７５は、公開鍵無効化リストＣＲＬに相手（ＩＣカード２１０ａ）のＩＤが含まれているか否かチェックする。

【００５６】楕円曲線暗号処理部２７６は、ＳＡＣにおける認証等の際に、楕円曲線にしたがった暗号処理（例えば、２５６ｂｉｔの処理単位）を実行する。

【００５７】認証部２７７は、ＳＡＣを介してＩＣカード２１０ａと通信する通信インタフェースである。

【００５８】バッファメモリ２７８は、乱数生成部２７４が生成した乱数や、楕円曲線暗号処理部２７６が生成した一時的なデータを保持する。

【００５９】次いで、ＩＣカード２１０ａおよびデスクランブラ２６０間のＳＡＣ設定、並びに、ＤＶＤ２ａに記録された暗号化コンテンツを復号化のシーケンスを図５に基づいて説明する。図５は、ＩＣカード２１０ａおよびデスクランブラ２６０により行われる通信シーケン

ス図である。

【００６０】ユーザ操作によるＤＶＤ２ａのコンテンツ再生指示があると、デスクランブラ２６０の乱数生成部２７４は、第１の乱数ｙ（例えば、１２８ビット）を生成し、これをバッファメモリ２７８に格納する（Ｓ１）。そして、デスクランブラ２６０の認証部２７７は、バッファメモリ２７８に格納された第１の乱数ｙと、デスクランブラ用公開鍵証明書記憶部２７３に記憶されたデスクランブラ用公開鍵証明書Ｃｅｒｔ＿ｉとを読み出して、これらをＩＣカード２１０ａに送信する（Ｓ２）。

【００６１】ＩＣカード２１０ａの認証部２３７は、デスクランブラ２６０から受信した第１の乱数ｙとデスクランブラ用公開鍵証明書Ｃｅｒｔ＿ｉとをバッファメモリ２３８に格納する。そして、公開鍵無効化リストチェック部２３５は、ＨＤ－ＤＶＤプレーヤ２００ａから渡された公開鍵無効化リストＣＲＬに基づいて、デスクランブラ２６０がＲｅｖｏｋｅされていないかどうかチェックする（Ｓ３）。具体的には、公開鍵無効化リストＣＲＬにデスクランブラ２６０のＩＤが掲載されているか否かで判断する。Ｒｅｖｏｋｅされていない場合には、認証部２３７は、公開鍵認証局の公開鍵ＰＫ＿ＣＡで、デスクランブラ用公開鍵証明書Ｃｅｒｔ＿ｉの検証を行う（Ｓ４）。具体的には、デスクランブラ用公開鍵証明書Ｃｅｒｔ＿ｉに含まれる公開鍵認証局の署名を公開鍵認証局の公開鍵ＰＫ＿ＣＡで解読し、デスクランブラ用公開鍵証明書Ｃｅｒｔ＿ｉが確かにデスクランブラ２６０のものであるか否か検証する。検証が終わると、乱数生成部２３４は、第１の乱数ｘ（例えば、１２８ビット）を生成し、生成した第１の乱数ｘをバッファメモリ２３８に格納する（Ｓ５）。そして、認証部２３７は、バッファメモリ２３８に格納された第１の乱数ｘと、ＩＣカード用公開鍵証明書記憶部２３３に記憶されたＩＣカード用公開鍵証明書Ｃｅｒｔ＿Ａとを読み出して、これらをデスクランブラ２６０に送信する（Ｓ６）。

【００６２】デスクランブラ２６０においては、ＩＣカード２１０ａから受信した第１の乱数ｘと、ＩＣカード用公開鍵証明書Ｃｅｒｔ＿Ａとを、認証部２７７によりバッファメモリ２７８に格納させた後、公開鍵無効化リストチェック部２７５は、ＨＤ－ＤＶＤプレーヤ２００ａから渡された公開鍵無効化リストＣＲＬに基づいて、ＩＣカード２１０ａがＲｅｖｏｋｅされていないかどうかをチェックする（Ｓ７）。具体的には、公開鍵無効化リストＣＲＬにＩＣカード２１０ａのＩＤが掲載されているか否かで判断する。Ｒｅｖｏｋｅされていない場合には、認証部２７７は、公開鍵証明書認証局の公開鍵ＰＫ＿ＣＡを用いて、ＩＣカード用公開鍵証明書Ｃｅｒｔ＿Ａの検証を行う（Ｓ８）。具体的には、プレーヤメーカ用公開鍵証明書Ｃｅｒｔ＿Ａに含まれる公開鍵認証局の署名を公開鍵認証局の公開鍵ＰＫ＿ＣＡで解読し、ＩＣカード用公開鍵証明書Ｃｅｒｔ＿Ａが確かにＩＣカード２１０ａのものであるか否か検証する。検証が終わると乱数生成部２７４は、第２の乱数ｙ’（例えば、１２８ビット）を生成し、この第２の乱数ｙ’をバッファメモリ２７８に格納する（Ｓ９）。そして、楕円曲線暗号処理部２７６は、第２の乱数ｙ’とベースポイントＧ（定数）とを楕円曲線上で乗算し、乗算の結果ｙ’Ｇを生成し、この乗算の結果ｙ’Ｇをバッファメモリ２７８に記憶する（Ｓ１０）。次いで、認証部２７７は、乗算の結果ｙ’Ｇに対する署名Ｓ１：＝Ｓｉｇ（ＳＫ＿ｉ，ｙ’Ｇ||ｘ）を生成し、この署名Ｓ１をバッファメモリ２７８に記憶する（Ｓ１１）。この署名は、乗算の結果ｙ’Ｇに第１の乱数ｘをビット連結したものに対して、秘密鍵ＳＫ＿ｉで署名することにより行われる。なお、記号「||」は、ビット連結を表し、ｙ’Ｇと、乱数ｘを桁方向に結合して２５６ビット（例えば、ｙ’Ｇを上位１２８ビット、乱数ｘを下位１２８ビット）とすることを示している。署名Ｓ１の記憶が終わると、認証部２７７は、乗算結果ｙ’Ｇと、これに対する署名Ｓ１とをＩＣカード２１０ａに送る（Ｓ１２）。

【００６３】ＩＣカード２１０ａの認証部２３７は、ｙ’Ｇと、これに対する署名Ｓ１とをバッファメモリ２３８に記憶した後、デスクランブラ用公開鍵証明書Ｃｅｒｔ＿ｉにより入手したデスクランブラ用公開鍵ＰＫ＿ｉを用いて、Ｓ１がｙ’Ｇ||ｘに対するデスクランブラ２６０の署名であることを検証する（Ｓ１３）。具体的には署名Ｓ１をデスクランブラ用公開鍵ＰＫ＿ｉで解読し、ｙ’Ｇと乱数ｘとのビット連結を分離したりして、検証する。これにより、通信相手（デスクランブラ２６０）が盗聴者等でないことを確認することができる。

【００６４】このような検証が終わると、ＩＣカード２１０ａの乱数生成部２３４は、第２の乱数ｘ’を生成し、バッファメモリ２３８に記憶する（Ｓ１４）。次いで、楕円曲線暗号処理部２３６は、第２の乱数ｘ’とベースポイントＧ（定数）とを楕円曲線上で乗算し、乗算の結果ｘ’Ｇを生成し、これをバッファメモリ２３８に記憶する（Ｓ１５）。次いで、認証部２３７は、乗算の結果ｘ’Ｇに対する署名Ｓ０：＝Ｓｉｇ（ＳＫ＿Ａ，ｘ’Ｇ||ｙ）を生成し、この署名Ｓ０をバッファメモリ２３８に記憶する（Ｓ１６）。この署名は、乗算の結果ｘ’Ｇに第１の乱数ｙをビット連結したものを、秘密鍵ＳＫ＿Ａで署名することにより行われる。署名の記憶が終わると、認証部２３７は、乗算結果ｘ’Ｇと署名Ｓ０とをデスクランブラ２６０に送る（Ｓ１７）。

【００６５】デスクランブラ２６０の認証部２７７は、ＩＣカード２１０ａから受け取った乗算結果ｘ’Ｇと署名Ｓ０とをバッファメモリ２７８に記憶させた後、ＩＣカード用公開鍵証明書Ｃｅｒｔ＿Ａにより入手したＩＣカード用公開鍵ＰＫ＿Ａを用いて、Ｓ０がｘ’Ｇ||ｙに対するデスクランブラ２６０の署名であることを検証す

る（Ｓ１８）。具体的には署名Ｓ１をデスクランブラ用公開鍵ＰＫ＿ｉで解読し、ｙ’Ｇと乱数ｘとのビット連結を分離したりして、検証する。これにより、通信相手（ＩＣカード２１０ａ）が盗聴者等でないことを確認することができる。

【００６６】デスクランブラ２６０の認証部２７７は、ＩＣカード２１０ａがＲｅｖｏｋｅされておらず、盗聴者等でもないことの確認が済むと、バッファメモリ２７８に記憶した自己側で生成した第２の乱数ｙ’（例えば、１２８ビット）と、通信相手からもらった乗算結果ｘ’Ｇとの乗算Ｋ’＝ｙ’（ｘ’Ｇ）を計算により生成し、計算結果Ｋ’をセッション鍵としてバッファメモリ２７８に格納する（Ｓ１９）。

【００６７】一方、ＩＣカード２１０ａの認証部２３７は、デスクランブラ２６０がＲｅｖｏｋｅされておらず、盗聴者等でもないことの確認が済むと、バッファメモリ２３８に記憶されている自己側で生成した第２の乱数ｘ’と、通信相手からもらった乗算結果ｙ’Ｇとの乗算Ｋ：＝ｘ’（ｙ’Ｇ）を計算により生成し、計算結果Ｋをセッション鍵としてバッファメモリ２３８に格納する（Ｓ２０）。これにより、ＩＣカード２１０ａとデスクランブラ２６０とは、同じ値の鍵Ｋ（＝Ｋ’）を持ち合うことができ、以降、Ｋ（＝Ｋ’）をセッション鍵として、暗号通信を行う（Ｓ２１）。

【００６８】セッション鍵Ｋの生成が終わると、ＩＣカード２１０ａのコンテンツ鍵復号部２２０ａは、コンテンツ鍵復号化処理を実行する。このコンテンツ鍵復号化処理においては、先ずハッシュ関数処理部２２２は、ＨＤ－ＤＶＤプレーヤ２００ａから渡された公開鍵無効化リストＣＲＬのハッシュ値Ｈａｓｈを計算する（Ｓ２２）。次いで、Ｅｘ－ＯＲ部２２３は、証明書認証局用公開鍵記憶部２３１に記憶されたＩＣカード２１０ａ自身のデバイス鍵ＫＤ＿Ａとハッシュ値Ｈａｓｈとの排他的論理和をとる（Ｓ２３）。Ｄｅｃ処理部２２４は、得られた排他的論理和値で、暗号化コンテンツ鍵を復合化し、コンテンツ鍵Ｋｃを取得し（Ｓ２４）、このコンテンツ鍵Ｋｃを認証部２３７に渡してコンテンツ鍵復号化処理を終了する。認証部２３７は、コンテンツ鍵Ｋｃが渡されると、このコンテンツ鍵Ｋｃをセッション鍵Ｋで暗号化し（Ｓ２５）、ＳＡＣ経由で、デスクランブラ２６０に送信する（Ｓ２６）。これにより、コンテンツ鍵Ｋｃの盗聴等が確実に防がれる。

【００６９】デスクランブラ２６０の認証部２７７は、ＩＣカード２１０ａから受信した暗号化コンテンツ鍵をセッション鍵Ｋ’で復号化し、コンテンツ鍵Ｋｃを取得し（Ｓ２７）、取得したコンテンツ鍵ＫｃをＤｅｃ処理部２８０に渡す。デスクランブラ２６０は、暗号化されたコンテンツを認証部２７７から渡されたコンテンツ鍵Ｋｃで復号化し、コンテンツを取得する（Ｓ２８）。これにより、著作権保護を図りつつコンテンツの復号化が可能になる。

【００７０】ここで、ＩＣカード２１０ａ、デスクランブラ２６０に対して、ＨＤ－ＤＶＤプレーヤ２００ａが、ＤＶＤ２ａにバインドされた公開鍵証明書無効化リストＣＲＬの代わりに、自己の公開鍵が無効になる前の公開鍵証明書無効化リストＣＲＬにすり替えて渡した場合を想定する。この場合には、すり替えがなかった場合と同様に、ＳＡＣ設定がされ、セッション鍵による暗号通信の段階（Ｓ２１）までは進むことができる。

【００７１】しかしながら、本実施の形態１では、公開鍵証明書無効化リストＣＲＬと、この公開鍵証明書無効化リストＣＲＬのハッシュ値Ｈａｓｈを関与させた情報で暗号化された暗号化コンテンツ鍵の束とをＤＶＤ２ａにバインドするようにしている。このため、ＣＲＬのすり替えが行われたような場合、すり替えた公開鍵証明書無効化リストＣＲＬのハッシュ値ＨａｓｈとＤＶＤ２ａにバインドされた公開鍵証明書無効化リストＣＲＬのハッシュ値Ｈａｓｈとは、その値が一致しない。この結果、すり替えた公開鍵証明書無効化リストＣＲＬのハッシュ値Ｈａｓｈを用いてコンテンツ鍵を復号しようとしても、正規のコンテンツ鍵Ｋｃを取得できない。このため、コンテンツを復号するためのコンテンツ鍵Ｋｃを得るためには、ＤＶＤ２ａにバインドされた公開鍵証明書無効化リストＣＲＬを渡さなければならなくなる。したがって、公開鍵証明書無効化リストＣＲＬのすり替えを行うような悪質な復号化装置２００ａを排除することができ、著作権の保護を強化することができる。

【００７２】（実施の形態２）図６は、本実施の形態２に係る記録メディア用著作権保護システム１ｂの全体構成を示す機能ブロック図である。なお、この記録メディア用著作権保護システム１ｂにおいて、実施の形態１の記録メディア用著作権保護システム１ａと対応する部分に同じ番号を付し、その説明を省略し、記録メディア用著作権保護システム１ａの場合との異同を中心に説明する。

【００７３】実施の形態１に係る暗号化装置１００ａの端末装置１１０ａでは、ハッシュ関数処理部１１４から出力された公開鍵証明書無効化リストＣＲＬのハッシュ値Ｈａｓｈと各デバイス鍵との排他的論理和値をＥｘ－ＯＲ部１１５により算出し、Ｅｎｃ部１１６において、コンテンツ鍵Ｋｃをその排他的論理和値で暗号化し、暗号化コンテンツ鍵の束を生成していた。これに対して実施の形態２の暗号化装置１００ｂの端末装置１１０ｂにおいては、Ｅｎｃ部１１７においてコンテンツ鍵Ｋｃをデバイス鍵束記憶部１１２に記憶された各デバイス鍵だけで暗号化し、各デバイス鍵だけで暗号化された暗号化コンテンツ鍵の束を生成するように構成されている。

【００７４】また、実施の形態１に係る暗号化装置１００ａの端末装置１１０ａは、コンテンツ鍵Ｋｃをそのまま端末装置１６０に渡していた。このため、端末装置１

６０では、Ｅｎｃ部１６２においてコンテンツをコンテンツ鍵Ｋｃで暗号化し、暗号化コンテンツを生成していた。これに対して、実施の形態２の暗号化装置１００ｂの端末装置１１０ｂにおいては、Ｅｘ－ＯＲ部１１８により、ハッシュ関数処理部１１４から出力された公開鍵証明書無効化リストＣＲＬのハッシュ値Ｈａｓｈとコンテンツ鍵Ｋｃとの排他的論理和をとり、その排他的論理和値を端末装置１６０に渡すように構成されている。このため、その排他的論理和値を受け取った端末装置１６０では、Ｅｎｃ部１６２においてコンテンツをその排他的論理和値で暗号化し、暗号化コンテンツを生成する。

【００７５】したがって、ＤＶＤ２ｂにバインドされた各暗号化コンテンツ鍵にはハッシュ値が関与しておらず、暗号化コンテンツにはハッシュ値が関与しており、ＤＶＤ２ａの場合と逆の関係となる。また、実施の形態１に係る復号化装置２００ａのコンテンツ鍵復号部２２０ａでは、Ｅｘ－ＯＲ部２２３においてデバイス鍵記憶部２２１に記憶された自己のデバイス鍵ＫＤ＿Ａと公開鍵証明書無効化リストＣＲＬのハッシュ値Ｈａｓｈとの排他的論理和値を算出し、Ｄｅｃ処理部２２４において、ハッシュ値が関与した暗号化コンテンツ鍵をその排他的論理和値で復号し、コンテンツ鍵Ｋｃを取得していた。

【００７６】これに対して、実施の形態２に係る復号化装置２００ｂのコンテンツ鍵復号部２２０ｂでは、ＤＶＤ２ｂにバインドされた暗号化コンテンツ鍵にハッシュ値Ｈａｓｈが関与していないため、Ｄｅｃ処理部２２５において暗号化コンテンツ鍵をデバイス鍵記憶部２２１に記憶された自己のデバイス鍵だけで復号化し、コンテンツ鍵Ｋｃを取得するように構成されている。そして、ＤＶＤ２ｂにバインドされた暗号化コンテンツにハッシュ値Ｈａｓｈが関与しているため、Ｅｘ－ＯＲ部２２６において、Ｄｅｃ処理部２２５により取得されたコンテンツ鍵Ｋｃと、ハッシュ関数処理部２２２により算出された公開鍵証明書無効化リストＣＲＬのハッシュ値Ｈａｓｈとの排他的論理和値を算出し、得られた排他的論理和値を認証処理部２３０ａの認証部２３７に渡すように構成されている。

【００７７】このコンテンツ鍵Ｋｃと、ハッシュ値Ｈａｓｈとの排他的論理和値は、認証部２３７から、ＳＡＣ、デスクランブラ２６０の認証部２７７を介してＤｅｃ処理部２８０に渡される。このため、Ｄｅｃ処理部２８０は、ＤＶＤ２ｂに記録されたハッシュ値Ｈａｓｈが関与した暗号化コンテンツを、コンテンツ鍵Ｋｃとハッシュ値Ｈａｓｈとの排他的論理和値で復号化し、コンテンツを取得する。

【００７８】したがって、この実施の形態２に係る記録メディア用著作権保護システム１ｂにおいても、実施の形態１の場合と同様に、コンテンツを復号するための鍵を得るためには、ＤＶＤ２ａにバインドされた公開鍵証明書無効化リストＣＲＬを渡さなければならなくなる。この結果、公開鍵証明書無効化リストＣＲＬのすり替えを行うような不正な復号化装置２００ｂを排除でき、著作権の保護を強化することができる。

【００７９】（実施の形態３）図７は、本実施の形態３に係る記録メディア用著作権保護システム１ｃの全体構成を示す機能ブロック図である。なお、同図においては、実施の形態１の記録メディア用著作権保護システム１ａと対応する機能部分の図示が省略され、この記録メディア用著作権保護システム１ｃに特有の機能部分のみが図示されている。

【００８０】実施の形態１に係る復号化装置２００ｃのＩＣカード２１０ａは、取得したコンテンツ鍵Ｋｃをデスクランブラ２６０ｂに単純に渡すだけであり、ＩＣカード２１０ａ自身では、取得したコンテンツ鍵Ｋｃが暗号化コンテンツを正常に復号化できる正規の鍵かどうかがわからなかった。このため、取得したコンテンツ鍵Ｋｃをデスクランブラ２６０に渡す前に、この内部でコンテンツ鍵Ｋｃが正しい値であるかどうかを予めチェックすることが望ましい。

【００８１】そこで、この本実施の形態３に係る記録メディア用著作権保護システム１ｃは、このような鍵チェック機能を有するシステムであって、暗号化装置１００ｃの著作権保護ライセンサが使用する端末装置端末装置１１０ｃは、端末装置１１０ａの構成に加えて、さらに、固定パターン記憶部１１９を備える。この固定パターン記憶部１１９は、予め定められた固定パターン平文（例えば、１６進で表される固定パターン平文「０１２３４５６７８９ＡＢＣＤＥＦ」）をコンテンツ鍵Ｋｃで暗号化した固定パターンを予め記憶する。この固定パターン記憶部１１９に記憶された固定パターンは、端末装置１６０を介してＤＶＤ２ｃにバインドされる。

【００８２】その一方、復号化装置２００ｃのＩＣカード２１０ｃに設けられるコンテンツ鍵復号部２２０ｃは、コンテンツ鍵復号部２２０ａの構成に加えてさらにＤｅｃ処理部２２７と、コンテンツ復号鍵チェック部２２８とを備える。Ｄｅｃ処理部２２７は、ＤＶＤ２ａにバインドされた固定パターン平文の暗号化データをＤｅｃ処理部２２４により復号化されたコンテンツ鍵Ｋｃで復号化する。コンテンツ復号鍵チェック部２２８は、上記の固定パターン平文「０１２３４５６７８９ＡＢＣＤＥＦ」を予め保持しており、予め保持している固定パターン平文と、Ｄｅｃ処理部２２７により復号化された固定パターン平文とが同じであるか否かで復号化されたコンテンツ鍵Ｋｃが正しい値であるかどうかをチェックする。

【００８３】このように構成された記録メディア用著作権保護システム１ｃによれば、ＩＣカード２１０ｃの内部でコンテンツ鍵Ｋｃが正しい値であるかどうかを予めチェックすることができ、デスクランブラ２６０におけ

41

る誤ったコンテンツ鍵Ｋｃを用いたコンテンツ復号化という無駄な復号化処理を事前に回避することができる。なお、この実施の形態３の記録メディア用著作権保護システム１ｃにおいては、鍵チェック機能を実施の形態１の記録メディア用著作権保護システム１ａに適用したが、実施の形態２に係る記録メディア用著作権保護システム１ｂに適用してもよい。

【００８４】その場合には、コンテンツがコンテンツ鍵Ｋｃと公開鍵証明書無効化リストＣＲＬのハッシュ値Ｈａｓｈとの排他的論理和値で暗号化されているので、固定パターン記憶部１１９に固定パターン平文「０１２３４５６７８９ＡＢＣＤＥＦ」をコンテンツ鍵Ｋｃとハッシュ値Ｈａｓｈとの排他的論理和値で暗号化した固定パターンを予め記憶し、この固定パターンをＤＶＤ２ｃに記録すればよい。

【００８５】一方、コンテンツ鍵復号部２２０ｃのＤｅｃ処理部２２７では、Ｄｅｃ処理部２２４の出力、すなわちコンテンツ鍵Ｋｃに代えてＥｘ－ＯＲ部２２６（図６参照）の出力、すなわちコンテンツ鍵Ｋｃとハッシュ値Ｈａｓｈとの排他的論理和値でＤＶＤ２ａにバインドされた固定パターン平文の暗号化データを復号化すればよい。そして、コンテンツ復号鍵チェック部２２８で、予め保持している固定パターン平文「０１２３４５６７８９ＡＢＣＤＥＦ」と、Ｄｅｃ処理部２２７により復号化された固定パターン平文とが同じであるか否かで復号化されたコンテンツを復号するための鍵、すなわちコンテンツ鍵Ｋｃとハッシュ値Ｈａｓｈとの排他的論理和値が正しい値であるかどうかをチェックできる。

【００８６】（実施の形態４）図８は、本実施の形態４に係る記録メディア用著作権保護システム１ｄの全体構成を示す機能ブロック図である。なお、同図においても、実施の形態１の記録メディア用著作権保護システム１ａと対応する機能部分の図示が省略され、この記録メディア用著作権保護システム１ｄに特有の機能部分のみが図示されている。

【００８７】本実施の形態４に係る記録メディア用著作権保護システム１ｄは、記録メディア用著作権保護システム１ｃと同様に鍵チェック機能を有するシステムであって、暗号化装置１００ｄの端末装置１１０ｄは、端末装置１１０ａの構成に加えて、さらに、Ｅｎｃ部１３１を備える。このＥｎｃ部１３１は、コンテンツ鍵記憶部１１３から読み出されたコンテンツ鍵Ｋｃをこのコンテンツ鍵Ｋｃで暗号化したコンテンツ鍵照合データを生成する。このコンテンツ鍵照合データは、ＤＶＤ２ｄにバインドされる。

【００８８】一方、復号化装置２００ｄのＩＣカード２１０ｄに設けられるコンテンツ鍵復号部２２０ｄは、コンテンツ鍵復号部２２０ａの構成に加えてさらにＥｎｃ部２４１と、コンテンツ鍵チェック部２４２とを備える。Ｅｎｃ部２４１は、端末装置１１０ｄのＥｎｃ部１３１と同構成であって、Ｄｅｃ処理部２２４により復号化されたコンテンツ鍵Ｋｃを、そのコンテンツ鍵Ｋｃで暗号化し、コンテンツ鍵照合データを生成する。コンテンツ鍵チェック部２４２は、Ｅｎｃ部２４１により生成されたコンテンツ鍵照合データと、ＤＶＤ２ｄにバインドされたコンテンツ鍵照合データとを比較し、これらのデータが同じ値であるか否かで、Ｄｅｃ処理部２２４により復号化されたコンテンツ鍵Ｋｃが正しい鍵、すなわち暗号化コンテンツを復号できる鍵であるかどうかをチェックする。

【００８９】このように構成された記録メディア用著作権保護システム１ｄによっても、記録メディア用著作権保護システム１ｃと同様に、ＩＣカード２１０ｄの内部でコンテンツ鍵Ｋｃが正しい値であるかどうかを予めチェックすることができ、デスクランブラ２６０における誤ったコンテンツ鍵Ｋｃを用いたコンテンツ復号化という無駄な復号化処理を事前に回避することができる。なお、この実施の形態４の記録メディア用著作権保護システム１ｄにおいては、鍵チェック機能を実施の形態１の記録メディア用著作権保護システム１ａに適用したが、実施の形態２に係る記録メディア用著作権保護システム１ｂに適用してもよい。

【００９０】その場合には、コンテンツがコンテンツ鍵Ｋｃと公開鍵証明書無効化リストＣＲＬのハッシュ値Ｈａｓｈとの排他的論理和値で暗号化されているので、Ｅｎｃ部１３１においては、コンテンツ鍵記憶部１１３の出力、すなわちコンテンツ鍵Ｋｃに代えて、Ｅｘ－ＯＲ部１１８の出力、すなわちコンテンツ鍵Ｋｃとハッシュ値Ｈａｓｈとの排他的論理和値をこの排他的論理和値で暗号化し、このコンテンツ鍵照合データをＤＶＤ２ｃに記録すればよい。

【００９１】一方、コンテンツ鍵復号部２２０ｄのＥｎｃ部２４１では、Ｄｅｃ処理部２２４の出力、すなわちコンテンツ鍵Ｋｃに代えてＥｘ－ＯＲ部２２６（図６参照）の出力、すなわちコンテンツ鍵Ｋｃとハッシュ値Ｈａｓｈとの排他的論理和値をその排他的理和値で暗号化すればよい。そして、コンテンツ鍵チェック部２４２で、Ｅｎｃ部２４１により生成されたコンテンツ鍵照合データと、ＤＶＤ２ｄにバインドされたコンテンツ鍵照合データとを比較し、これらの鍵が同じ値であるか否かで、Ｅｘ－ＯＲ部２２６により生成された鍵が正しい鍵、すなわち暗号化コンテンツを復号できる鍵であるかどうかをチェックすることができる。

【００９２】（実施の形態５）図９は、本実施の形態５に係る記録メディア用著作権保護システム１ｅの全体構成を示す機能ブロック図である。なお、同図においても、実施の形態１の記録メディア用著作権保護システム１ａと対応する機能部分の図示が省略され、この記録メディア用著作権保護システム１ｅに特有の機能部分のみが図示されている。

42

【００９３】本実施の形態５に係る記録メディア用著作権保護システム１ｅは、記録メディア用著作権保護システム１ｃ，１ｄと同様に鍵チェック機能を有するシステムであって、実施の形態４と同じ構成の暗号化装置１００ｄで構成されており、ＤＶＤ２ｄには、Ｅｎｃ部１３１により生成されたコンテンツ鍵照合データがバインドされている。

【００９４】一方、復号化装置２００ｅのＩＣカード２１０ｅに設けられるコンテンツ鍵復号部２２０ｅは、コンテンツ鍵復号部２２０ａの構成に加えてさらにＤｅｃ処理部２４３と、コンテンツ復号鍵チェック部２４４とを備える。Ｄｅｃ処理部２４３は、上記のＥｎｃ部１３１により暗号化され、ＤＶＤ２ｄにバインドされたコンテンツ鍵照合データをＤｅｃ処理部２２４により復号化されたコンテンツ鍵Ｋｃで復号化する。コンテンツ復号鍵チェック部２４４は、Ｄｅｃ処理部２２４により復号化されたコンテンツ鍵Ｋｃと、Ｄｅｃ処理部２４３により復号化されたコンテンツ鍵Ｋｃとを比較し、これらの鍵が同じ値であるか否かで、Ｄｅｃ処理部２２４により復号化されたコンテンツ鍵Ｋｃが正しい鍵、すなわち暗号化コンテンツを復号できる鍵であるかどうかをチェックする。

【００９５】このように構成された記録メディア用著作権保護システム１ｅによっても、メディア用著作権保護システム１ｃ，１ｄと同様に、ＩＣカード２１０ｅの内部でコンテンツ鍵Ｋｃが正しい値であるかどうかを予めチェックすることができ、デスクランブラ２６０における誤ったコンテンツ鍵Ｋｃを用いたコンテンツ復号化という無駄な復号化処理を事前に回避することができる。

【００９６】なお、この実施の形態５の記録メディア用著作権保護システム１ｅにおいては、鍵チェック機能を実施の形態１の記録メディア用著作権保護システム１ａに適用したが、実施の形態２に係る記録メディア用著作権保護システム１ｂに適用してもよい。

【００９７】この場合には、コンテンツがコンテンツ鍵Ｋｃと公開鍵証明書無効化リストＣＲＬのハッシュ値Ｈａｓｈとの排他的論理和値で暗号化されているので、実施の形態４の変形例と同様に、Ｅｎｃ部１３１においては、コンテンツ鍵記憶部１１３の出力、すなわちコンテンツ鍵Ｋｃに代えて、Ｅｘ－ＯＲ部１１８の出力、すなわちコンテンツ鍵Ｋｃとハッシュ値Ｈａｓｈとの排他的論理和値をこの排他的論理和値で暗号化し、この暗号化により生成されたコンテンツ鍵照合データをＤＶＤ２ｃに記録すればよい。

【００９８】一方、コンテンツ鍵復号部２２０ｅのＤｅｃ処理部２４３では、ＤＶＤ２ｃから読み出したコンテンツ鍵復号データを、Ｄｅｃ処理部２２４の出力、すなわちコンテンツ鍵Ｋｃに代えてＥｘ－ＯＲ部２２６（図６参照）の出力、すなわちコンテンツ鍵Ｋｃとハッシュ値Ｈａｓｈとの排他的論理和値で復号化する。そして、

コンテンツ復号鍵チェック部２４４において、Ｅｘ－ＯＲ部２２６により復号化されたコンテンツを復号化するための鍵、すなわちコンテンツ鍵Ｋｃとハッシュ値Ｈａｓｈとの排他的論理和と、Ｄｅｃ処理部２４３により復号化された鍵とを比較し、これらの鍵が同じ値であるか否かで、Ｅｘ－ＯＲ部２２６により復号化された鍵が正しい鍵、すなわち暗号化コンテンツを復号できる鍵であるかどうかをチェックすればよい。

【００９９】（実施の形態６）図１０は、本実施の形態６に係る記録メディア用著作権保護システム１ｆの全体構成を示す機能ブロック図である。上述の記録メディア用著作権保護システム１ａ～１ｅでは、ＤＶＤにバインドされた公開鍵証明書無効化リストＣＲＬを公開鍵無効化リストチェック部２３５でチェックし、通信相手（デスクランブラ２６０）がＲｅｖｏｋｅされているか否か判断していた。このようなチェックでは、ＤＶＤの製造時期が古い、すなわちＤＶＤにバインドされた公開鍵証明書無効化リストＣＲＬが古いと、この公開鍵証明書無効化リストＣＲＬの更新日以降に通信相手（デスクランブラ２６０）の公開鍵証明書が無効化されたような場合、このデスクランブラ２６０をＲｅｖｏｋｅすることができない。このため、できるだけ最新版の公開鍵証明書無効化リストＣＲＬを使用して、通信相手（デスクランブラ２６０）がＲｅｖｏｋｅされているか否か判断する必要がある。

【０１００】そこで、この本実施の形態６に係る記録メディア用著作権保護システム１ｆにおいては、復号化装置２００ｆのＩＣカード２１０ｆに係る認証処理部２３０ｂに、認証処理部２３０ａの構成に加えてさらに公開鍵無効化リスト最新版記憶処理部２３９が設けられている。

【０１０１】この公開鍵無効化リスト最新版記憶処理部２３９は、今までに受け取った公開鍵証明書無効化リストＣＲＬ中の最新版を復号化装置２００ｆ側で記憶して保持するための処理部であって、最新版検出処理部２３９１と、最新版検出情報記憶部２３９２と、記憶部２３９３等とからなる。

【０１０２】最新版検出処理部２３９１は、ＤＶＤ２ａにバインドされた公開鍵証明書無効化リストＣＲＬを受け取るごとに、この公開鍵証明書無効化リストＣＲＬが最新版か否かの確認判断の処理等を行う。

【０１０３】最新版検出情報記憶部２３９２は、この復号化装置２００ｆ側で保持する公開鍵証明書無効化リストＣＲＬの最新版検出情報（例えば、このリストのファイルサイズ）を記憶する。

【０１０４】記憶部２３９３は、復号化装置２００ｆ側で保持する公開鍵証明書無効化リストＣＲＬのハッシュ値（例えば、１２８ビット）を記憶する。その理由は、膨大な量となる公開鍵証明書無効化リストＣＲＬ自体をＩＣカード２１０ｆ内で記憶・保持したのでは、ＩＣカ

ード２１０ｆのコストアップになり得るので、それを回避するためにである。つまり、この実施の形態では、ＩＣカード２１０ｆの外（かつ、復号化装置２００ｆの中）に、公開鍵証明書無効化リスト最新版記憶部２５０を設け、この公開鍵証明書無効化リスト最新版記憶部２５０に最新版の公開鍵証明書無効化リストＣＲＬ本体を記憶させ、このリストのハッシュ値だけをＩＣカード２１０ｆ内の記憶部２３９３で記憶・保持する構成を採用している。そして、公開鍵無効化リストチェック部２３５により通信相手が無効化されている機器かどうかのチェックを行う場合に、最新版の公開鍵証明書無効化リストＣＲＬをＩＣカード２１０ｆ内に読み出し、読み出した公開鍵証明書無効化リストＣＲＬが改ざんされていないか否かをハッシュ値でチェックしている。

【０１０５】具体的には、ＤＶＤ２ａにバインドされた新たな公開鍵証明書無効化リストＣＲＬを受け取ると、その公開鍵証明書無効化リストＣＲＬを保存しておく（又は、保存しないでおく）ための処理として、最新版検出処理部２３９１は、先ず、図１１（ａ）のフローチャートに示されるように、公開鍵証明書無効化リストＣＲＬが最新版か否かの確認判断の処理を実行する。つまり、最新版検出処理部２３９１は先ず、ＤＶＤ２ａにバインドされた公開鍵証明書無効化リストＣＲＬのヘッダに記録されたファイルサイズと、最新版検出情報記憶部２３９２に記憶しているファイルサイズとを比較する（Ｓ１０１）。この比較は、時が経つにつれて無効化される機器の台数が単調増加するだけであり、ファイルサイズも大きくなるという公開鍵証明書無効化リストＣＲＬの性質を根拠としている。

【０１０６】その結果、ＤＶＤ２ａにバインドされた公開鍵証明書無効化リストＣＲＬのファイルサイズの方が大きい場合（Ｓ１０１でＹｅｓ）、すなわち、今ＤＶＤ２ａから読み込んだ公開鍵証明書無効化リストＣＲＬの方が最新である場合、この最新版リストのファイルサイズを最新版検出情報記憶部２３９２に格納（上書き）して更新する（Ｓ１０２）。次いで最新版検出処理部２３９１は、最新版リストのハッシュ値を算出して、算出したハッシュ値を記憶部２３９３に格納し（Ｓ１０３）、最新版リストを外部の公開鍵証明書無効化リスト最新版記憶部２５０に格納し（Ｓ１０４）、公開鍵無効化リストチェック部２３５に最新版リストを転送して（Ｓ１０５）、確認判断処理を終了する。

【０１０７】一方、ＤＶＤ２ａにバインドされた公開鍵証明書無効化リストＣＲＬのファイルサイズの方が大きくない場合（Ｓ１０１でＮｏ）、すなわち、今ＤＶＤ２ａから読み込んだ公開鍵証明書無効化リストＣＲＬの方が最新でない場合、最新版検出処理部２３９１は、確認判断処理を直ちに終了する。そして、もし、最新の公開鍵証明書無効化リストＣＲＬが必要な場合には、図１１（ｂ）のフローチャートに示される最新版リスト読み出し処理を実行する。

【０１０８】その読み出し処理においては、最新版検出処理部２３９１は、先ず、最新版リストを外部の記憶部、すなわち公開鍵証明書無効化リスト最新版記憶部２５０から読み出し（Ｓ１１１）、最新版リストのハッシュ値を算出し（Ｓ１１２）、算出したハッシュ値と記憶部２３９３に記憶されているハッシュ値とが一致するか否かを判断する（Ｓ１１３）。この判断は、公開鍵証明書無効化リストＣＲＬがＩＣカード２１０ｆの外部ですり替えが行われたか否かを検出するために行われ、すり替えがなかった場合には、ハッシュ値は一致する。

【０１０９】ハッシュ値が一致する場合（Ｓ１１３でＹｅｓ）、最新版検出処理部２３９１は、公開鍵証明書無効化リスト最新版記憶部２５０から読み出した最新版リストを公開鍵無効化リストチェック部２３５に転送して（Ｓ１１４）、最新版リスト読み出し処理を終了する。これに対してハッシュ値が一致しない場合（Ｓ１１３でＮｏ）、最新版検出処理部２３９１は、処理を中止して（Ｓ１１５）、最新版リスト読み出し処理を終了する。なお、ハッシュ値が一致しないために最新の公開鍵証明書無効化リストＣＲＬを読み出すことができなかった場合には、何らかの不正行為が行われたものとして、例えば、公開鍵証明書無効化リストＣＲＬを用いる以降の全ての処理を中止（相手装置の認証を拒絶）する。

【０１１０】このように、実施の形態６の記録メディア用著作権保護システム１ｆによれば、ＤＶＤ２ａから読み出された公開鍵証明書無効化リストＣＲＬのうち、最新のものだけが公開鍵証明書無効化リスト最新版記憶部２５０に保持され、利用されるので、古い公開鍵証明書無効化リストＣＲＬを用いて相手装置を認証してしまう不具合が回避される。なお、この実施の形態６においては、最新版リストの確認方法としてファイルサイズを用いたが、この変形例として、公開鍵証明書無効化リストＣＲＬに登録されている証明書の件数（シリアル番号のエントリー数）で最新版リストか否かの確認をしてもよい。

【０１１１】次に、本発明に係る著作権保護システムの実施の形態である記録媒体用の復号化装置２００ａ～２００ｆをＨＤ－ＤＶＤプレーヤに適用した例について、図面を用いて説明する。図１２は、本発明の実施の形態に係る記録媒体用の復号化装置２００ａ～２００ｆを備えるＨＤ－ＤＶＤプレーヤの外観図である。このＨＤ－ＤＶＤプレーヤ２００は、ＤＶＤ２ａ～２ｄに記録された映画等のコンテンツをＩＣカード２１０ａ～２１０ｆを用いて再生するシステムであり、ＩＣカード２１０ａ～２１０ｆが装着されるカード挿入口２１００、ＤＶＤ２ａ～２ｄを再生するＤＶＤ－ＲＯＭドライブ２２００、ＨＤ－ＤＶＤプレーヤ２００の本体内部に実装されるデスクランブラ２６０等から構成される。

【０１１２】なお、ＩＣカード２１０ａ～２１０ｆは、

プラスチック製のカードにＣＰＵを含むＩＣチップが埋め込まれたカードであり、内蔵されたＣＰＵによる処理により、データの読み書きの際のアクセスが正当なものであるかどうかを判断できる。そのため、外部からの不正なアクセスや改ざんを行うことが非常に困難であり、高いセキュリティを実現できる。

【０１１３】本発明に係る暗号化装置をこのような映像再生システムに適用することで、ＤＶＤ２ａ～２ｄに記録されたデジタル著作物は不正コピー等から保護され、マルチメディア関連製品の流通市場における健全な発展が期待できる。

【０１１４】（実施の形態７）図１３は、本実施の形態７に係る記録メディア用著作権保護システム１ｇの全体構成を示す機能ブロック図である。なお、この記録メディア用著作権保護システム１ｇにおいて、実施の形態１の記録メディア用著作権保護システム１ａと対応する部分に同じ番号を付し、その説明を省略し、記録メディア用著作権保護システム１ａとの異同を中心に説明する。

【０１１５】ところで、実施の形態１に係る暗号化装置１００ａでは、２つの鍵、デバイス鍵ＫＤ＿Ａの束と、コンテンツ鍵Ｋｃとをデバイス鍵束記憶部１１２、コンテンツ鍵記憶部１１３にそれぞれ記憶しておき、コンテンツ鍵Ｋｃを、公開鍵無効化リストＣＲＬのハッシュ値を関与させたデバイス鍵ＫＤ＿Ａの束で暗号化し、暗号化コンテンツ鍵の束を生成し、コンテンツをコンテンツ鍵Ｋｃで暗号化し、暗号化コンテンツ鍵を生成していた。すなわち、デバイス鍵ＫＤ＿Ａと、コンテンツ鍵Ｋｃとで、秘密鍵を２層化している。このような秘密鍵の２層化で、通常は、アタックに対する暗号強度が十分にある。

【０１１６】しかしながら、暗号強度をさらに向上させて欲しいというライセンサもある。そこで、本実施の形態７の暗号化装置１００ｅの端末装置１１０ｅにおいては、秘密鍵を上記したデバイス鍵ＫＤ＿Ａおよびコンテンツ鍵Ｋｃに、ディスク鍵Ｋｄをさらに加えた３層化した構成を採用し、暗号強度をさらに向上させている。

【０１１７】すなわち、暗号化装置１００ｅの端末装置１１０ｅは、公開鍵無効化リスト記憶部１１１、デバイス鍵束記憶部１１２、コンテンツ鍵記憶部１１３、ハッシュ関数処理部１１４、Ｅｘ－ＯＲ部１１５の他に、さらに、ディスク鍵Ｋｄを予め記憶するハッシュ関数処理部１１４と、Ｅｎｃ部１４２，１４３とを備えている。なお、このディスク鍵Ｋｄは、１枚のＤＶＤに複数（７個程度）のコンテンツが入ることを考慮し、コンテンツごとのコンテンツ鍵の上位に設けられる秘密鍵である。

【０１１８】Ｅｎｃ部１４２は、ディスク鍵記憶部１４１に記憶されたディスク鍵Ｋｄをハッシュ値Ｈａｓｈと各デバイス鍵ＫＤ＿Ａとの排他的論理和値で暗号化し、暗号化ディスク鍵の束を生成する。

【０１１９】Ｅｎｃ部１４３は、コンテンツ鍵記憶部１１３に記憶されたコンテンツ鍵Ｋｃをディスク鍵Ｋｄで暗号化し、暗号化コンテンツ鍵を生成する。

【０１２０】このため、端末装置１６０は、ＤＶＤ２ｅに対して、暗号化コンテンツや、公開鍵証明書無効化リストＣＲＬの他、上記Ｅｎｃ部１４２，１４３により生成された暗号化ディスク鍵の束と、暗号化コンテンツ鍵とをバインドさせる。これに応じて、復号化装置２００ｇのＩＣカード２１０ｇのコンテンツ鍵復号部２２０ｆは、デバイス鍵ＫＤ＿Ａだけを記憶し、ＤＶＤ２ｅにバインドされた暗号化ディスク鍵の束をデバイス鍵ＫＤ＿Ａと公開鍵無効化リストＣＲＬのハッシュ値とで復号化することにより、ディスク鍵Ｋｄを復号化し、さらに、ＤＶＤ２ｅにバインドされた暗号化コンテンツ鍵をディスク鍵Ｋｄで復号化することにより、コンテンツ鍵Ｋｃを復号化する。すなわち、コンテンツ鍵復号部２２０ｆは、デバイス鍵記憶部２２１、ハッシュ関数処理部２２２、Ｅｘ－ＯＲ部２２３の他に、Ｄｅｃ処理部２４５，２４６を備えている。

【０１２１】Ｄｅｃ処理部２４５は、デスクランブラ２６０から渡された暗号化ディスク鍵の束をデバイス鍵ＫＤ＿Ａと公開鍵無効化リストＣＲＬのハッシュ値とで復号化することにより、ディスク鍵Ｋｄを復号化する。

【０１２２】Ｄｅｃ処理部２４６は、デスクランブラ２６０から渡された暗号化コンテンツ鍵をディスク鍵Ｋｄで復号化することにより、コンテンツ鍵Ｋｃを復号化する。したがって、この実施の形態７に係る記録メディア用著作権保護システム１ｇにおいても、実施の形態１の場合と同様に、コンテンツを復号するための鍵を得るためには、ＤＶＤ２ｅにバインドされた公開鍵証明書無効化リストＣＲＬを渡さなければならなくなり、公開鍵証明書無効化リストＣＲＬのすり替えを行うような不正なデスクランブラ２６０を排除できるだけでなく、秘密鍵が３層化されているので、アタックに対する暗号強度が増加し、さらに著作権の保護を強化することができる。なお、この実施の形態では、秘密鍵を３層化したが、さらに多層化する構成で実施してもよい。この場合には、アタックに対する暗号強度をさらに増加させることができる。

【０１２３】また、端末装置１１０ｅに、さらに、復号化装置２００ｇにおいて復号化されたコンテンツ鍵が正しいものであるか否かを確認するための基準となる確認データをＤＶＤ２ｅに出力する確認データ出力部を備える構成としてもよい。この確認データ出力部は、所定の固定パターンのデータをコンテンツ鍵記憶部１１３に記憶されたコンテンツ鍵で暗号化して得られるデータを確認データとしてＤＶＤ２ｅに出力する構成であってもよく、また、確認データ出力部は、コンテンツ鍵をコンテンツ鍵で暗号化して得られるデータを確認データとしてＤＶＤ２ｅに出力する構成でもよい。また、この端末装置１１０ｅに対応して、コンテンツ鍵復号部２２０ｆ

に、復号したコンテンツ鍵が正しい鍵であるか否かを判定するコンテンツ復号鍵チェック部２２８、コンテンツ鍵チェック部２４２、コンテンツ復号鍵チェック部２４４等を備える構成としてもよい。

【０１２４】（実施の形態８）図１４は、本実施の形態８に係る記録メディア用著作権保護システム１ｈの全体構成を示す機能ブロック図である。なお、この記録メディア用著作権保護システム１ｈにおいて、実施の形態７の記録メディア用著作権保護システム１ｇと対応する部分に同じ番号を付し、その説明を省略し、記録メディア用著作権保護システム１ｇとの異同を中心に説明する。

【０１２５】ところで、実施の形態７に係る暗号化装置１００ｅの端末装置１１０ｅでは、ディスク鍵記憶部１４１に記憶されたディスク鍵Ｋｄをハッシュ値Ｈａｓｈと各デバイス鍵ＫＤ＿Ａとの排他的論理和値で暗号化し、暗号化ディスク鍵の束を生成するとともに、コンテンツ鍵記憶部１１３に記憶されたコンテンツ鍵Ｋｃをディスク鍵Ｋｄで暗号化し、暗号化コンテンツ鍵を生成する。この結果、端末装置１１０ｅでは、アタックに対する暗号強度が増加する反面、２つの暗号化処理のための負荷が大きい。また、コンテンツ鍵復号部２２０ｆにおいても、２つの復号化処理のための負荷も大きい。

【０１２６】そこで、本記録メディア用著作権保護システム１ｈの暗号化装置１００ｆに係る端末装置１１０ｆでは、コンテンツ鍵記憶部１１３に代えてＤＶＤごとに固有のメディアＩＤ、ＭＩＤを記憶するメディアＩＤ記憶部１４４と、Ｅｎｃ部１４３に代えてメディアＩＤ、ＭＩＤとディスク鍵Ｋｄとに基づいてコンテンツ鍵Ｋｃを生成する一方向関数部１４５とを用い、コンテンツ鍵Ｋｃを暗号化する処理を省くことにより、端末装置１１０ｆの付加の軽減を図っている。すなわち、暗号化装置１００ｆの端末装置１１０ｆは、公開鍵無効化リスト記憶部１１１、デバイス鍵束記憶部１１２、ハッシュ関数処理部１１４、Ｅｘ－ＯＲ部１１５、ディスク鍵記憶部１４１、Ｅｎｃ部１４２の他に、さらにメディアＩＤ記憶部１４４と、一方向関数部１４５とを備えている。

【０１２７】一方向関数部１４５は、例えばＥｘ－ＯＲであって、メディアＩＤ記憶部１４４に記憶されたメディアＩＤ、ＭＩＤとディスク鍵Ｋｄとを一方向関数に代入することにより、コンテンツ鍵Ｋｃを生成する。このコンテンツ鍵Ｋｃを生成する処理は、図１３のＥｎｃ部１４３による暗号化コンテンツ鍵を生成する処理に比べて負荷が軽い。

【０１２８】端末装置１６０は、ＤＶＤ２ｆに対して、公開鍵無効化リストＣＲＬ、暗号化コンテンツの他、上記Ｅｎｃ部１４２により生成された暗号化ディスク鍵の束と、メディアＩＤ記憶部１４４から出力されたメディアＩＤ、ＭＩＤとをバインドさせる。

【０１２９】これに応じて、復号化装置２００ｈのＩＣカード２１０ｈのコンテンツ鍵復号部２２０ｇは、デバイス鍵ＫＤ＿Ａだけを記憶し、ＤＶＤ２ｅにバインドされた暗号化ディスク鍵の束をデバイス鍵ＫＤ＿Ａと公開鍵無効化リストＣＲＬのハッシュ値とで復号化することにより、ディスク鍵Ｋｄを復号化し、さらに、ＤＶＤ２ｅにバインドされたメディアＩＤ、ＭＩＤとディスク鍵Ｋｄとに基づいて、コンテンツ鍵Ｋｃを生成する。すなわち、コンテンツ鍵復号部２２０ｇは、デバイス鍵記憶部２２１、ハッシュ関数処理部２２２、Ｅｘ－ＯＲ部２２３、Ｄｅｃ処理部２４５の他に、さらに一方向関数部１４５と同構成の一方向関数部２４７を備えている。

【０１３０】一方向関数部２４７は、メディアＩＤ、ＭＩＤをディスク鍵Ｋｄで一方向関数処理することにより、コンテンツ鍵Ｋｃを生成する。このコンテンツ鍵Ｋｃを生成する処理は、図１３のＤｅｃ処理部２４６によるコンテンツ鍵Ｋｃを復号化する処理に比べて負荷が軽い。ここで、メディアＩＤ、ＭＩＤはＤＶＤ２ｆにバインドされるので容易に知られるが、一方向関数部１４５，２４７の構成は秘密鍵と同様に知られにくい。

【０１３１】したがって、この実施の形態８に係る記録メディア用著作権保護システム１ｈにおいても、実施の形態１の場合と同様に、コンテンツを復号するための鍵を得るためには、ＤＶＤ２ａにバインドされた公開鍵証明書無効化リストＣＲＬを渡さなければならなくなり、公開鍵証明書無効化リストＣＲＬのすり替えを行うような不正なデスクランブラ２６０を排除できるだけでなく、暗号の強度が増すため、アタックに対する暗号強度が増加し、さらに著作権の保護を強化することができ、しかも端末装置１１０ｆおよびコンテンツ鍵復号部２２０ｇの負荷軽減することができる。

【０１３２】なお、端末装置１１０ｆに、さらに、復号化装置２００ｈにおいて復号化されたコンテンツ鍵が正しいものであるか否かを確認するための基準となる確認データをＤＶＤ２ｆに出力する確認データ出力部を備える構成としてもよい。この確認データ出力部は、所定の固定パターンのデータをコンテンツ鍵記憶部１１３に記憶されたコンテンツ鍵で暗号化して得られるデータを確認データとしてＤＶＤ２ｆに出力する構成であってもよく、また、確認データ出力部は、コンテンツ鍵をコンテンツ鍵で暗号化して得られるデータを確認データとしてＤＶＤ２ｆに出力する構成でもよい。また、この端末装置１１０ｆに対応して、コンテンツ鍵復号部２２０ｆに、復号したコンテンツ鍵が正しい鍵であるか否かを判定するコンテンツ復号鍵チェック部２２８、コンテンツ鍵チェック部２４２、コンテンツ復号鍵チェック部２４４等を備える構成としてもよい。

【０１３３】（実施の形態９）図１５は、本実施の形態９に係る記録メディア用著作権保護システム１ｉの一部構成を示す機能ブロック図である。なお、この記録メディア用著作権保護システム１ｉにおいて、実施の形態１の記録メディア用著作権保護システム１ａと対応する部

分に同じ番号を付し、その説明を省略し、記録メディア用著作権保護システム１ａとの異同を中心に説明する。

【０１３４】ところで、ＤＶＤというメディアは、パーソナルコンピュータ（ＰＣ）でも読み込むことができ、ＰＣとの親和性が高く、ＰＣにＤＶＤドライブを装着すると同時に、再生ソフトをハードディスク等にインストールしておき、このＰＣをＨＤ－ＤＶＤと同様に復号化装置として使用し、コンテンツを視聴することが行われている。この場合においても、ＤＶＤドライブが不正を働く場合が考えられ、ＨＤ－ＤＶＤの場合と同様に、著作権の保護を図る必要がある。

【０１３５】一方、実施の形態１では、ＩＣカード２１０ａとデスクランブラ２６０とで復号化装置２００ａを構成していたが、ＰＣの場合には、ＤＶＤドライブと再生ソフトとで復号化装置を構成するのか一般的である。そこで、この実施の形態９では、デスクランブラ２６０の認証処理部２７０の部分をＤＶＤドライブ４００に含ませ、ＩＣカード２１０ａとデスクランブラ２６０のＤｅｃ処理部２８０の部分をＤＶＤ再生ＰＣソフト５００に含ませることにより、復号化装置２００ｉを構成している。なお、ＤＶＤドライブ４００の製造元とＤＶＤ再生ＰＣソフト５００の販売元とは異なる。

【０１３６】ＤＶＤドライブ４００は、認証処理部２７０と略同構成であり、バス認証用公開鍵証明書記憶部４１０と、バス認証用秘密鍵記憶部４２０と、公開鍵復号部４３０と、鍵計算部４４０と、バス暗号部４５０とを備えている。

【０１３７】ＤＶＤドライブ４００のバス認証用公開鍵証明書記憶部４１０は、ＩＤＥバスやＳＣＳＩバス等のバス認証用の公開鍵証明書を予め記憶しており、ＤＶＤ２ａのコンテンツ再生に際して、バス認証用の公開鍵証明書をＤＶＤ再生ＰＣソフト５００に渡す。

【０１３８】バス認証用秘密鍵記憶部４２０～バス暗号部４５０は、セッション鍵Ｋを生成し、ＤＶＤ再生ＰＣソフト５００との間でＳＡＣを形成するものである。

【０１３９】ＤＶＤ再生ＰＣソフト５００は、その機能として、証明書正当性検査部５１０と、公開鍵有効性検査部５２０と、公開鍵暗号部５３０と、検証部５４０と、鍵計算部５５０と、バス復号部５６０と、ハッシュ関数処理部５７０と、デバイス鍵記憶部５８０と、Ｄｅｃ処理部５９０，５９５とを備える。このような各部は、ソフトと、ＰＣのＣＰＵ、メモリ等により実現される。

【０１４０】証明書正当性検査部５１０は、バス認証用公開鍵証明書記憶部４１０から送られてきた証明書を公開鍵で解読し、証明書が正当なものかどうか検査する。

【０１４１】公開鍵有効性検査部５２０は、証明書正当性検査部５１０から証明書が正当である旨の通知を受けると、ＤＶＤドライブ４００を介して受け取ったバス認証用公開鍵無効化リストＣＲＬと、公開鍵証明書無効化

リスト最新版記憶部２５０から読み出した最新のバス認証用公開鍵無効化リストＣＲＬとを参照し、ＤＶＤドライブ４００がＲｅｖｏｋｅされていないかどうか検査する。

【０１４２】公開鍵暗号部５３０～バス復号部５６０は、公開鍵有効性検査部５２０からＤＶＤドライブ４００がＲｅｖｏｋｅされていない、すなわち、ＤＶＤドライブ４００が正当である旨の通知を受けると、セッション鍵Ｋ’を生成し、ＤＶＤドライブ４００との間でＳＡＣを形成する部分である。

【０１４３】公開鍵暗号部５３０は、公開鍵証明書無効化リストＣＲＬのハッシュ値Ｈａｓｈを算出する。

【０１４４】デバイス鍵記憶部５８０は、デバイス鍵ＫＤ＿Ａを予め記憶する。

【０１４５】Ｄｅｃ処理部５９０は、バス復号部５６０から出力された暗号化コンテンツ鍵と、ハッシュ関数処理部５７０から出力されたハッシュ値Ｈａｓｈと、デバイス鍵ＫＤ＿Ａとに基づいて、コンテンツ鍵Ｋｃを生成する。Ｄｅｃ処理部５９０は、ＤＶＤ２ａにバインドされた暗号化コンテンツをコンテンツ鍵Ｋｃで復号化し、コンテンツを生成する。

【０１４６】次いで、ＤＶＤドライブ４００とＤＶＤ再生ＰＣソフト５００との間で行われる認証の処理等を説明する。公開鍵暗号部５３０は、ＤＶＤドライブ４００が正当である旨を通知を受け取ると、乱数ｃｈａを生成し、生成した乱数ｃｈａを相手のバス認証用公開鍵で暗号化し、ＤＶＤドライブ４００の公開鍵復号部４３０に暗号化した乱数ｃｈａを転送する。

【０１４７】公開鍵復号部４３０は、暗号化された乱数ｃｈａを、バス認証用秘密鍵記憶部４２０に記憶されているバス認証用秘密鍵で解読し、乱数ｃｈａを取得する。そして、公開鍵復号部４３０は、乱数ｃｈａと自己の秘密鍵とを相手のバス認証用公開鍵で暗号化し、暗号化結果を検証部５４０に転送すると供に、乱数ｃｈａと秘密鍵とを鍵計算部４４０に渡す。鍵計算部４４０は、乱数ｃｈａと秘密鍵とに基づいてセッション鍵Ｋを計算し、セッション鍵Ｋをバス暗号部４５０に渡す。バス暗号部４５０は、暗号化コンテンツ鍵の束をセッション鍵Ｋで暗号化し、２重に暗号化されたコンテンツ鍵の束をＤＶＤ再生ＰＣソフト５００に送る。

【０１４８】一方、ＤＶＤ再生ＰＣソフト５００の検証部５４０は、自己の秘密鍵を用いて、復号により得られた乱数ｃｈａが元の乱数ｃｈａと一致するかを確認し、一致していれば、乱数ｃｈａと、相手の秘密鍵とを鍵計算部５５０に渡す。鍵計算部５５０は、乱数ｃｈａと、相手の秘密鍵とを用いてセッション鍵Ｋ’を計算し、バス復号部５６０に渡す。バス復号部５６０は、２重に暗号化されたコンテンツ鍵の束をセッション鍵Ｋ’で復号化し、暗号化コンテンツ鍵の束を生成し、暗号化コンテンツ鍵の束をＤｅｃ処理部５９０に出力する。

【０１４９】他方、ハッシュ関数処理部５７０は、ＤＶＤドライブ４００を介して出力されたＣＲＬのハッシュ値Ｈａｓｈを算出し、ハッシュ値ＨａｓｈをＤｅｃ処理部５９０に出力する。Ｄｅｃ処理部５９０は、例えば、暗号化コンテンツ鍵の束とハッシュ値Ｈａｓｈとの排他的論理和を算出することにより、コンテンツ鍵ＫｃをデバイスＫＤ＿Ａで暗号化した値に復号化し、これをさらにデバイス鍵ＫＤ＿Ａで復号化することにより、コンテンツ鍵Ｋｃを復号化し、コンテンツ鍵ＫｃをＤｅｃ処理部５９５に渡す。Ｄｅｃ処理部５９５は、ＤＶＤ２ａにバインドされた暗号化コンテンツをコンテンツ鍵Ｋｃで復号化し、コンテンツを再生する。

【０１５０】したがって、この実施の形態９に係る記録メディア用著作権保護システムＩｉの復号化装置２００ｉ、すなわち、ＤＶＤドライブ４００とＤＶＤ再生ＰＣソフト５００で構成されたＰＣであっても、ＨＤ－ＤＶＤと同様に、コンテンツを復号するための鍵を得るためには、ＤＶＤ２ａにバインドされた公開鍵証明書無効化リストＣＲＬを渡さなければならなくなり、公開鍵証明書無効化リストＣＲＬのすり替えを行うような不正なデスクランブラ２６０を排除でき、著作権の保護を図ることができる。

【０１５１】なお、復号化装置２００ｉ、すなわちＰＣがインターネットに接続されているような場合には、ＤＶＤ２ｅの再生の際に端末装置３００にアクセスし、端末装置３００から最新のＣＲＬをダウンロードし、ダウンロードした最新のＣＲＬを用いて、ＤＶＤドライブ４００がＲｅｖｏｋｅされているか否かを公開鍵有効性検査部５２０で検査してもよい。

【０１５２】また、実施の形態９の復号化装置２００ｉでは、ＤＶＤドライブ４００と、ＤＶＤ再生ＰＣソフト５００で構成したが、実際にはＤＶＤ再生ＰＣソフトも、いわゆる「デスクランブル」機能しか有せず、ライセンサ供給保護モジュールＡをつないで使用する場合も想定される。すなわち、ＰＣにＩＣカード２１０ａを装着できるようにし、このＰＣにより構成される復号化装置２００ｉをＤＶＤドライブ４００と、ＩＣカード２１０ａと、Ｄｅｃ処理部５９５部分のＤＶＤ再生ＰＣソフトとで構成してもよい。

【０１５３】この場合には、ＤＶＤドライブ４００とＩＣカード２１０ａとでＳＡＣを形成し、ＩＣカード２１０ａと、Ｄｅｃ処理部５９５部分のＤＶＤ再生ＰＣソフトとでＳＡＣを形成した後、ＤＶＤドライブ４００により読み出された暗号化コンテンツをコンテンツ鍵で復号化し、コンテンツを再生すればよい。

【０１５４】また、暗号化装置１００ａに、さらに、復号化装置２００ｉにおいて復号化されたコンテンツ鍵が正しいものであるか否かを確認するための基準となる確認データをＤＶＤ２ａに出力する確認データ出力部を備える構成とし、この確認データ出力部は、所定の固定パターンのデータをコンテンツ鍵記憶部１１３に記憶されたコンテンツ鍵で暗号化して得られるデータを確認データとしてＤＶＤ２ｆに出力する構成又は、確認データ出力部は、コンテンツ鍵をコンテンツ鍵で暗号化して得られるデータを確認データとしてＤＶＤ２ｆに出力する構成である場合、この端末装置１１０ａに対応して、コンテンツ鍵復号部２２０ｉに、復号したコンテンツ鍵が正しい鍵であるか否かを判定するコンテンツ復号鍵チェック部２２８、コンテンツ鍵チェック部２４２、コンテンツ復号鍵チェック部２４４等を備える構成としてもよい。

【０１５５】以上、本発明に係る著作権保護システムについて、実施の形態に基づいて説明したが、本発明は、これらの実施の形態に限定されるものではない。例えば、上記実施の形態における著作権保護システムでは、ＤＶＤという記録媒体を介してデジタル著作物が転送されたが、インターネット等の伝送媒体を介してデジタル著作物を転送するシステムに本発明を適用することができる。つまり、記録媒体への記録に代えて伝送路への送信とし、記録媒体からの読み出しに代えて伝送路からの受信とすることで、本発明に係る著作権保護システムを適用することができる。

【０１５６】また、記録媒体と伝送媒体とを組み合わせてデジタル著作物を転送するシステムにも本発明を適用することができる。つまり、例えば暗号化コンテンツについてはＤＶＤという記録媒体で提供し、暗号化コンテンツを復号化するための鍵や、ＣＲＬ等については伝送媒体によるネット配信で提供してもよい。また、この逆の形、すなわち、鍵等については記録媒体で提供し、暗号化コンテンツについては伝送媒体によるネット配信で提供してもよい。この記録媒体と伝送媒体とを組み合わせてデジタル著作物を転送するシステムにおいては、暗号化コンテンツや鍵等の内、何を記録媒体で提供し、何を伝送媒体によるネット配信で提供するかは、任意に定めることができる。

【０１５７】また、上記実施の形態では、著作権保護モジュール（耐タンパモジュール）をＩＣカード２１０ａ～２１０ｆで実施したが、図１６に示されるように、ＩＣカード２１０ａ～２１０ｆの各機能構成を１チップに集積化したＬＳＩ２１０ｉで構成してもよく、このＬＳＩ２１０ｉをソケット２１０ｊに装着したり、半田等で基板に直付けして装着するようにしてもよい。また、上記実施の形態では、ＩＣカード２１０ａ～２１０ｆを著作権保護ライセンサが供給するものとして説明したが、この復号化装置２００ａ～２００ｆの製造メーカが製造したＩＣカード２１０ａ～２１０ｆやＬＳＩ２１０ｉであってもよい。

【０１５８】また、上記実施の形態においては、著作権保護ライセンサやコンテンツ製造メーカの暗号化装置１００ａ～１００ｆとユーザが使用する復号化装置２００

55

ａ～２００ｆとの間の広域で本発明に係る著作権保護システムを適用する場合について説明したが、家庭内や一企業内等狭いエリアにおいてデジタル著作物であるコンテンツを暗号化通信する際の処理に、本著作権保護システムを適用することができる。

【０１５９】（実施の形態１０）図１７は小規模のホームＬＡＮを介してコンテンツを暗号化通信する著作権保護システムの全体構成を示すブロック図であり、図１８は図１７に示されるＡＶサーバ１００ｊ及び各プラズマＴＶ２００ｋ，ＶＴＲ２００ｍ，ＤＶＤレコーダ２００ｎの構成を示すブロック図である。なお、図１８においては、プラズマＴＶ２００ｋ，ＶＴＲ２００ｍ，ＤＶＤレコーダ２００ｎの構成が著作権保護機構部分について同じであるので、これらの代表例としてプラズマＴＶ２００ｋの構成のみが図示されている。

【０１６０】この著作権保護システム１ｊは、転送媒体としてのホームＬＡＮ３０と、このホームＬＡＮ３０に接続されるＡＶサーバ１００ｊと、クライアントとしてのプラズマＴＶ２００ｋ，ＶＴＲ２００ｍ，ＤＶＤレコーダ２００ｎとから構成される。

【０１６１】ＡＶサーバ１００ｊは、図１に示される暗号化装置１００ａとほぼ同様に構成されているものの、家庭外部から受信したコンテンツをＨＤＤ等により構成されるコンテンツ記憶部１６１に蓄積し、プラズマＴＶ２００ｋ，ＶＴＲ２００ｍ，ＤＶＤレコーダ２００ｎからの蓄積コンテンツ配信要求に応じて要求されたコンテンツ等をホームＬＡＮ３０を介してネット配信する点が、暗号化装置１００ａの場合と大きく異なっている。

【０１６２】より詳しくは、ＡＶサーバ１００ｊは、放送局１００ｇから衛星放送（ＢＳ，ＣＳ）や、地上波放送の放送網３ａを介してコンテンツを受信したり、コンテンツプロバイダのサーバ１００ｈからインターネット網３ｂを介してコンテンツを受信したり、ＣＡＴＶ局１００ｉからＣＡＴＶ網３ｃを介してコンテンツを受信したりし、受信したコンテンツをコンテンツ記憶部１６１に蓄積する。

【０１６３】そして、ＡＶサーバ１００ｊは、セッション鍵記憶部１１２ａを備えており、クライアントのいずれか、例えばプラズマＴＶ２００ｋからコンテンツ記憶部１６１に蓄積している蓄積コンテンツの配信要求があった場合、この配信要求に基づいてプラズマＴＶ２００ｋとの間でＳＡＣを形成し、ＳＡＣ形成の際に得られたセッション鍵Ｋｓｅｓをセッション鍵記憶部１１２ａに格納し、暗号化装置１００ａで用いられていたデバイス鍵に代えてセッション鍵Ｋｓｅｓを用いてコンテンツ鍵Ｋｃを暗号化する点が、デバイス鍵を用いてコンテンツ鍵Ｋｃを暗号化する暗号化装置１００ａの場合と大きく異なっている。即ち、デバイス鍵に代替してセッション鍵Ｋｓｅｓが用いられる点が、暗号化装置１００ａの場合と大きく異なっている。

56

【０１６４】一方、プラズマＴＶ２００ｋ，ＶＴＲ２００ｍ，ＤＶＤレコーダ２００ｎは、図１に示される復号化装置２００ａとほぼ同様に構成されているものの、ＡＶサーバ１００ｊとの間におけるＳＡＣ形成の際に得られたセッション鍵Ｋｓｅｓを記憶するためのセッション鍵記憶部２２１ａをそれぞれ備え、セッション鍵記憶部２２１ａに記憶されたセッション鍵Ｋｓｅｓを用いてコンテンツ鍵Ｋｃを復号化する点が、デバイス鍵ＫＤ＿Ａを用いてコンテンツ鍵Ｋｃを復号化する復号化装置２００ａの場合と大きく異なっている。即ち、デバイス鍵ＫＤ＿Ａに代替してセッション鍵Ｋｓｅｓが用いられる点が、復号化装置２００ａの場合と大きく異なっている。

【０１６５】次いで、この著作権保護システム１ｊのＡＶサーバ１００ｊとプラズマＴＶ２００ｋとで行われる処理について、著作権保護システム１ａとの相違点を中心に説明する。

【０１６６】ＡＶサーバ１００ｊは、クライアントであるＤＶＤレコーダ２００ｎからコンテンツ配信の要求があると、プラズマＴＶ２００ｋとの間で、楕円暗号を用いてＳＡＣ処理を行う。そして、同じ値のセッション鍵Ｋｓｅｓを相互に持ち合い、ＡＶサーバ１００ｊはセッション鍵記憶部１１２ａにセッション鍵Ｋｓｅｓを格納し、プラズマＴＶ２００ｋの著作権保護モジュール２１０ｋにおけるコンテンツ鍵復号部２２０ｈは、セッション鍵記憶部２２１ａにセッション鍵Ｋｓｅｓを格納する。次いで、ＡＶサーバ１００ｊのＥｘ－ＯＲ部１１５は、プラズマＴＶ２００ｋ間で共有されたセッション鍵Ｋｓｅｓと、ＣＲＬのハッシュ値とをＸＯＲする。そして、Ｅｎｃ部１１６は、Ｅｘ－ＯＲ部１１５によって得られた値を鍵として用いて、コンテンツ鍵Ｋｃを暗号化する。次いで、Ｅｎｃ部１６２は、コンテンツ鍵Ｋｃで，ＡＶデータの要求されたコンテンツを暗号化する。コンテンツ鍵及びコンテンツの暗号化が終わると、ＡＶサーバ１００ｊは、ＣＲＬと共に、暗号化コンテンツ鍵及び暗号化コンテンツをホームＬＡＮ３０を介してプラズマＴＶ２００ｋに送信する。

【０１６７】プラズマＴＶ２００ｋ内の著作権保護モジュール２１０ｋは、ホームＬＡＮ３０を介して送信されてきたＣＲＬ及び暗号化コンテンツ鍵を受信し、また、デスクランブラ２６０は、ＣＲＬ及び暗号化コンテンツを受信する。次いで、プラズマＴＶ２００ｋの著作権保護モジュール２１０ｋにおけるコンテンツ鍵復号部２２０ｈのＥｘ－ＯＲ部２２３は、セッション鍵記憶部２２１ａに記憶されているセッション鍵Ｋｓｅｓと、ハッシュ関数処理部２２２によって得られたＣＲＬのハッシュ値とをＸＯＲする。次いで、Ｄｅｃ処理部２２４は、Ｅｘ－ＯＲ部２２３によって得られた値を鍵として用いてコンテンツ鍵を復号化する。そして、プラズマＴＶ２００ｋ内の著作権保護モジュール２１０ｋと、デスクランブラ２６０との間で、送られてきたＣＲＬに基づいて、

57

ＳＡＣ処理を行い、セッション鍵ＫＫを共有する。

【０１６８】次いで、著作権保護モジュール２１０ｋの認証部２３７は、共有したセッション鍵ＫＫで、コンテンツ鍵Ｋｃを暗号化し、デスクランブラ２６０に送信し、デスクランブラ２６０の認証部２７７はコンテンツ鍵Ｋｃを復号化する。Ｄｅｃ処理部２８０は、入手したコンテンツ鍵Ｋｃにて、暗号化コンテンツを復号化する。したがって、家庭や企業等比較的小さなネットワークに接続されたクライアントにおいても容易にコンテンツ利用ができ、しかも、末端のクライアントまで著作権保護を徹底化することができる。

【０１６９】なお、本実施の形態１０においては、デバイス鍵に代えてセッション鍵Ｋｓｅｓを用いたが、ＡＶサーバ１００ｊとプラズマＴＶ２００ｋ間で、秘密鍵Ｋｓを予め共有しているものとしてもよい。この場合には、セッション鍵Ｋｓｅｓに代えて秘密鍵Ｋｓを用いればよい。また、復号化したコンテンツ鍵が正しい値かどうかを予め調べるために、上記した固定パターンをＣＲＬ等と共に送信し、著作権保護モジュール２１０ｋにおいて予め確認できるように構成してもよい。

【０１７０】また、本発明は、上記１０個の実施の形態における特徴的な処理を組み合わせることで、様々な暗号化装置や復号化装置を実現することができる。つまり、暗号化の場合であれば、（１）秘密鍵に対する暗号化やメディアＩＤに対する一方向関数による変換それぞれを層と呼んだ場合に、その層の数に関しては、２層にするか、３層にするかの選択が可能であり、（２）コンテンツの暗号化に用いる鍵に関しては、コンテンツ鍵にするか、メディアＩＤを一方向性関数で変換して得られる関数値にするかの選択が可能であり、（３）公開鍵無効化リストのハッシュ値を関与させる対象に関しては、デバイス鍵にするか、ディスク鍵にするか、コンテンツ鍵にするか、メディアＩＤにするか、セッション鍵にするか、メディアＩＤを一方向性関数で変換して得られる関数値にするかの選択が可能である。

【０１７１】したがって、それらの独立したパラメータ（１）、（２）、（３）それぞれの１つずつを任意に組み合わせることで、様々な形態の暗号化装置、復号化装置及びＩＣカードを実現することができる。また、上記秘密鍵等の暗号化（又は、復号化）の層数としては１～３に限定されるものではなく、３層を超えるものであってもよい。これらのバリエーションを考慮して本発明の暗号化装置、復号化装置及びＩＣモジュール（秘密鍵生成装置）を表現すると以下のように言うことができる。

【０１７２】つまり、コンテンツ鍵を使用する暗号化方法であれば、デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置において、ｎ（≧２）個の秘密鍵のうち、第１秘密鍵を用いてデジタル著作物を暗号化するとともに、第ｉ（２≦ｉ≦ｎ）秘密鍵を用いて第（ｉ－１）秘密鍵を暗号化するという暗号化の連鎖

58

を前記第１～第（ｎ－１）秘密鍵について繰り返し、暗号化された第１～第（ｎ－１）秘密鍵を前記媒体に出力する方法であって、前記第１～第ｎ秘密鍵の少なくとも１つを用いた暗号化においては、その暗号化に先立ち、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストの内容に依存する属性値を用いて秘密鍵を変形させておくことを特徴とする暗号化方法である。

【０１７３】また、メディアＩＤを使用する暗号化方法であれば、デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置において、ｎ（≧１）個の秘密鍵のうち、第１秘密鍵を用いて媒体識別情報を一方向性関数で変換した後に、変換された媒体識別情報でデジタル著作物を暗号化するとともに、前記ｎが２以上の場合に、第ｉ（２≦ｉ≦ｎ）秘密鍵を用いて第（ｉ－１）秘密鍵を暗号化するという暗号化の連鎖を前記第１～第（ｎ－１）秘密鍵について繰り返し、暗号化された第１～第（ｎ－１）秘密鍵を前記媒体に出力する方法であって、前記第１～第ｎ秘密鍵の少なくとも１つを用いた暗号化又は変換においては、（ｉ）その暗号化又は変換に先立ち、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストの内容に依存する属性値を用いて秘密鍵を変形させておくか、又は、（２）前記変換によって得られた媒体識別情報を前記属性値で変形させておくことを特徴とする暗号化方法である。また、コンテンツ鍵を使用する復号化方法であれば、暗号化されたデジタル著作物を復号化する復号化装置において、暗号化されたデジタル著作物とｎ（≧２）個の暗号化秘密鍵と無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストとを記録媒体又は伝送媒体を介して取得した後に、予め保持している秘密鍵を用いて前記ｎ個の暗号化秘密鍵のうちの第１暗号化秘密鍵を復号化し、得られた第１秘密鍵で第２暗号化秘密鍵を復号化するという復号化の連鎖を前記ｎ個の暗号化秘密鍵について繰り返し、最後の復号化で得られた第ｎ秘密鍵でデジタル著作物を復号化する方法であって、前記第１～第ｎ暗号化秘密鍵に対する復号化の少なくとも１つおいては、その復号化に先立ち、復号化に用いる秘密鍵を前記公開鍵無効化リストの内容に依存する属性値で変形させておくことを特徴とする復号化方法である。

【０１７４】また、メディアＩＤを使用する復号化方法であれば、暗号化されたデジタル著作物を復号化する復号化装置において、暗号化されたデジタル著作物と媒体識別情報とｎ（≧１）個の暗号化秘密鍵と無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストとを記録媒体又は伝送媒体を介して取得した後に、予め保持している秘密鍵を用いて前記ｎ個の暗号化秘密鍵のうちの第１暗号化秘密鍵を復号化し、前記ｎが２以上の場合に、前記復号化で得られた第１秘密鍵で第２暗号化秘密鍵を復号化するという復号化の連鎖を前記

59

ｎ個の暗号化秘密鍵について繰り返し、最後の復号化で得られた第ｎ秘密鍵を用いて前記媒体識別情報を一方向性関数で変換し、変換後の媒体識別情報をデジタル著作物を復号化する方法であって、前記第１～第ｎ暗号化秘密鍵に対する復号化及び前記媒体識別情報に対する変換の少なくとも１つおいては、（１）その復号化又は変換に先立ち、復号化又は変換に用いる秘密鍵を前記公開鍵無効化リストの内容に依存する属性値で変形させておくか、又は、（２）前記変換によって得られた媒体識別情報を前記属性値で変形させておくことを特徴とする復号化方法である。

【０１７５】

【発明の効果】以上の説明から明らかなように、本発明に係る暗号化装置は、デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、デジタル著作物を記憶するデジタル著作物記憶手段と、デジタル著作物の暗号化に用いられる第１秘密鍵を記憶する第１秘密鍵記憶手段と、暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第２秘密鍵を記憶する第２秘密鍵記憶手段と、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第２秘密鍵記憶手段に記憶された第２秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記変形手段により変形された第２秘密鍵で暗号化する第１暗号化手段と、前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記第１秘密鍵記憶手段に記憶された第１秘密鍵で暗号化する第２暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第１暗号化手段により暗号化された第１秘密鍵および前記第２暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする。

【０１７６】これによって、暗号化装置からは、暗号化されたデジタル著作物と、その暗号化に用いられた第１秘密鍵の暗号化されたもの（暗号化第１秘密鍵）と、公開鍵無効化リストとが出力されるが、その暗号化第１秘密鍵は、復号化装置に対応づけられた第２秘密鍵によって単に第１秘密鍵が暗号化されているのではなく、公開鍵無効化リストが関与した第２秘密鍵によって暗号化されている。したがって、これら暗号化デジタル著作物、暗号化第１秘密鍵および公開鍵無効化リストを受け取った復号化装置は、公開鍵無効化リストが差し替えられていた場合には、内部に有する第２秘密鍵に対する公開鍵無効化リストによる関与の内容が異なったものとなり、そのように変形された第２秘密鍵を用いて暗号化第１秘

60

密鍵を本来の第１秘密鍵に復号化することができず、したがって、暗号化デジタル著作物を正しく復号化することができない。よって、公開鍵無効化リストの差し替え攻撃に対する防御機能を有した安全なデジタル著作物の転送が可能となる。

【０１７７】ここで、前記暗号化装置は、さらに、前記復号化装置のおいて復号化された第１秘密鍵が正しいものであるか否かを確認するための基準となる確認データを前記記録媒体又は伝送媒体に出力する確認データ出力手段を備えてもよい。例えば、前記確認データ出力手段は、所定の固定パターンのデータを前記第１秘密鍵記憶手段に記憶された第１秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力したり、前記確認データ出力手段は、前記第１秘密鍵記憶手段に記憶された第１秘密鍵を当該第１秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力してもよい。

【０１７８】これによって、この暗号化装置から出力された暗号化デジタル著作物、暗号化第１秘密鍵および公開鍵無効化リストを受け取った復号化装置は、公開鍵無効化リストの差し替え攻撃を受けたか否か、つまり、正しい第１秘密鍵に復元することができたか否かを判断することができるので、誤った第１秘密鍵でデジタル著作物を復号化するという無駄な処理を事前に回避することが可能となる。

【０１７９】また、本発明に係る暗号化装置は、デジタル著作物であるデジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、デジタル著作物を記憶するデジタル著作物記憶手段と、デジタル著作物の暗号化に用いられる第１秘密鍵を記憶する第１秘密鍵記憶手段と、暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第２秘密鍵を記憶する第２秘密鍵記憶手段と、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記第２秘密鍵記憶手段に記憶された第２秘密鍵で暗号化する第１暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第１秘密鍵記憶手段に記憶された第１秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記変形手段により変形された第１秘密鍵で暗号化する第２暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第１暗号化手段により暗号化された第１秘密鍵および前記第２暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする。

61

【０１８０】これによって、暗号化装置からは、暗号化されたデジタル著作物と、その暗号化に用いられた第１秘密鍵の暗号化されたもの（暗号化第１秘密鍵）と、公開鍵無効化リストとが出力されるが、その暗号化デジタル著作物は、単に第１秘密鍵で暗号化されているのではなく、第１秘密鍵に公開鍵無効化リストを関与させた変形後の第１秘密鍵で暗号化されている。したがって、これら暗号化デジタル著作物、暗号化第１秘密鍵および公開鍵無効化リストを受け取った復号化装置は、公開鍵無効化リストが差し替えられていた場合には、復号化した第１秘密鍵に対する公開鍵無効化リストによる関与の内容が異なったものとなり、そのように変形された第１秘密鍵を用いて暗号化デジタル著作物を正しく復号化することができない。よって、公開鍵無効化リストの差し替え攻撃に対する防御機能を有した安全なデジタル著作物の転送が可能となる。

【０１８１】また、上述と同様に、第１秘密鍵に公開鍵無効化リストを関与させたものに関する確認データを添付して暗号化装置から出力することで、この暗号化装置から出力された暗号化デジタル著作物、暗号化第１秘密鍵および公開鍵無効化リストを受け取った復号化装置は、公開鍵無効化リストの差し替え攻撃を受けたか否か、つまり、デジタル著作物の暗号化に用いられた正しい秘密鍵に復元することができたか否かを判断することができるので、誤った秘密鍵でデジタル著作物を復号化するという無駄な処理を事前に回避することが可能となる。

【０１８２】また、本発明に係る暗号通信装置は、相手装置の公開鍵を用いて相手装置と暗号通信する装置であって、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する記憶手段と、新たな公開鍵無効化リストを取得する取得手段と、取得された公開鍵無効化リストのサイズと前記記憶手段に記憶されている公開鍵無効化リストのサイズとを比較し、取得された公開鍵無効化リストのサイズが大きい場合に、取得された公開鍵無効化リストを前記記憶手段に格納して更新する格納手段と、前記記憶手段に格納された公開鍵無効化リストを参照して相手装置の公開鍵の有効性を判断し、有効と判断した場合に、その公開鍵を用いて相手装置と暗号通信する通信手段とを備えることを特徴とする。同様に、上記格納手段に代えて、取得された公開鍵無効化リストに示された前記証明書の数と前記記憶手段に記憶されている公開鍵無効化リストに示された前記証明書の数とを比較し、取得された公開鍵無効化リストに示された前記証明書の数が大きい場合に、取得された公開鍵無効化リストを前記記憶手段に格納して更新する格納手段とすることもできる。

【０１８３】これによって、公開鍵証明書無効化リストに登録されている公開鍵証明書の件数は、時の経過とともに増加する一方であるので、暗号通信装置は、よりサイズの大きい（あるいは、より登録件数の多い）公開鍵証明書無効化リスト、すなわち、より最新の公開鍵証明書無効化リストを常に保持することが可能となる。

62

【０１８４】以上のように、本発明により、公開鍵証明書無効化リストの差し替えという攻撃に対しても安全にデジタル著作物を転送することが可能となり、インターネット等の伝送路やＤＶＤ等の記録媒体を介したデジタル著作物の配信や流通が活発になってきた今日において、その実用的価値は極めて高い。

【図面の簡単な説明】

【図１】本実施の形態１に係る記録メディア用著作権保護システムの全体構成を示す機能ブロック図である。

【図２】公開鍵証明書無効化リストＣＲＬの構成例を示す図である。

【図３】著作権保護ライセンサ用公開鍵証明書の構成例を示す図である。

【図４】プレーヤメーカ用公開鍵証明書の構成例を示す図である。

【図５】復号化装置２００ａのＩＣカード２１０ａおよびデスクランブラ２６０間で行われる処理のシーケンスを示す図である。

【図６】本実施の形態２に係る記録メディア用著作権保護システム１ｂの全体構成を示す機能ブロック図である。

【図７】本実施の形態３に係る記録メディア用著作権保護システム１ｃの全体構成を示す機能ブロック図である。

【図８】本実施の形態４に係る記録メディア用著作権保護システム１ｄの全体構成を示す機能ブロック図である。

【図９】本実施の形態５に係る記録メディア用著作権保護システム１ｅの全体構成を示す機能ブロック図である。

【図１０】本実施の形態６に係る記録メディア用著作権保護システム１ｆの全体構成を示す機能ブロック図である。

【図１１】図１１（ａ）は、図１０の最新版検出処理部２３９１により行われる確認判断処理のフローチャートであり、図１１（ｂ）は、最新版リスト読み出し処理のフローチャートである。

【図１２】上記実施の形態１～２に係る記録媒体用の復号化装置２００ａ～２００ｆをＨＤ－ＤＶＤプレーヤに適用した場合の外観図である。

【図１３】本実施の形態７に係る記録メディア用著作権保護システム１ｇの全体構成を示す機能ブロック図である。

【図１４】本実施の形態８に係る記録メディア用著作権保護システム１ｈの全体構成を示す機能ブロック図である。

【図１５】本実施の形態９に係る記録メディア用著作権

63

保護システム１ｉの全体構成を示す機能ブロック図である。

【図１６】著作権保護モジュールをＬＳＩで構成した場合の実装例を示す図である。

【図１７】小規模のホームＬＡＮを介してコンテンツを暗号化通信する著作権保護システムの全体構成を示すブロック図である。

【図１８】図１７に示されるＡＶサーバ１００ｊ及びプラズマＴＶ２００ｋの構成を示すブロック図である。

【符号の説明】

１ａ～１ｊ	著作権保護システム
２ａ～２ｆ	ＤＶＤ
３０	ホームＬＡＮ
１００ａ～１００ｆ	暗号化装置
１００ｊ	ＡＶサーバ
１１０ａ～１１０ｆ，１６０，３００	端末装置
１１１	公開鍵無効化リスト記憶部
１１２	デバイス鍵束記憶部
１１３	コンテンツ鍵記憶部
１１４，２２２	ハッシュ関数処理部
１１５，１１８，２２３，２２６	Ｅｘ－ＯＲ部
１１６，１１７，１３１，１４２，１４３，１６２，２４１	Ｅｎｃ部
１１９	固定パターン記憶部
１４４	メディアＩＤ記憶部
１４５，２４７	一方向関数部
１６１	コンテンツ記憶部

64

２００	ＨＤ－ＤＶＤプレーヤ
２００ａ～２００ｉ	復号化装置
２１０ａ～２１０ｈ	ＩＣカード
２１０	ＬＳＩ
２１０ｋ	著作権保護モジュール
２２０ａ～２２０ｉ	コンテンツ鍵復号部
２２１	デバイス鍵記憶部
２２２	ハッシュ関数処理部
２２４，２２５，２２７，２４３，２８０	Ｄｅｃ処理部
２２８，２４４	コンテンツ復号鍵チェック部
２４２	コンテンツ鍵チェック部
２３０，２７０	認証処理部
２３９	公開鍵無効化リスト最新版記憶処理部
２３９１	最新版検出処理部
２３９２	最新版検出情報記憶部
２３９３	記憶部
２５０	公開鍵証明書無効化リスト最新版記憶部
２６０	デスクランブラ
４００	ＤＶＤドライブ
５００	ＤＶＤ再生ＰＣソフト

【図２】

CRL

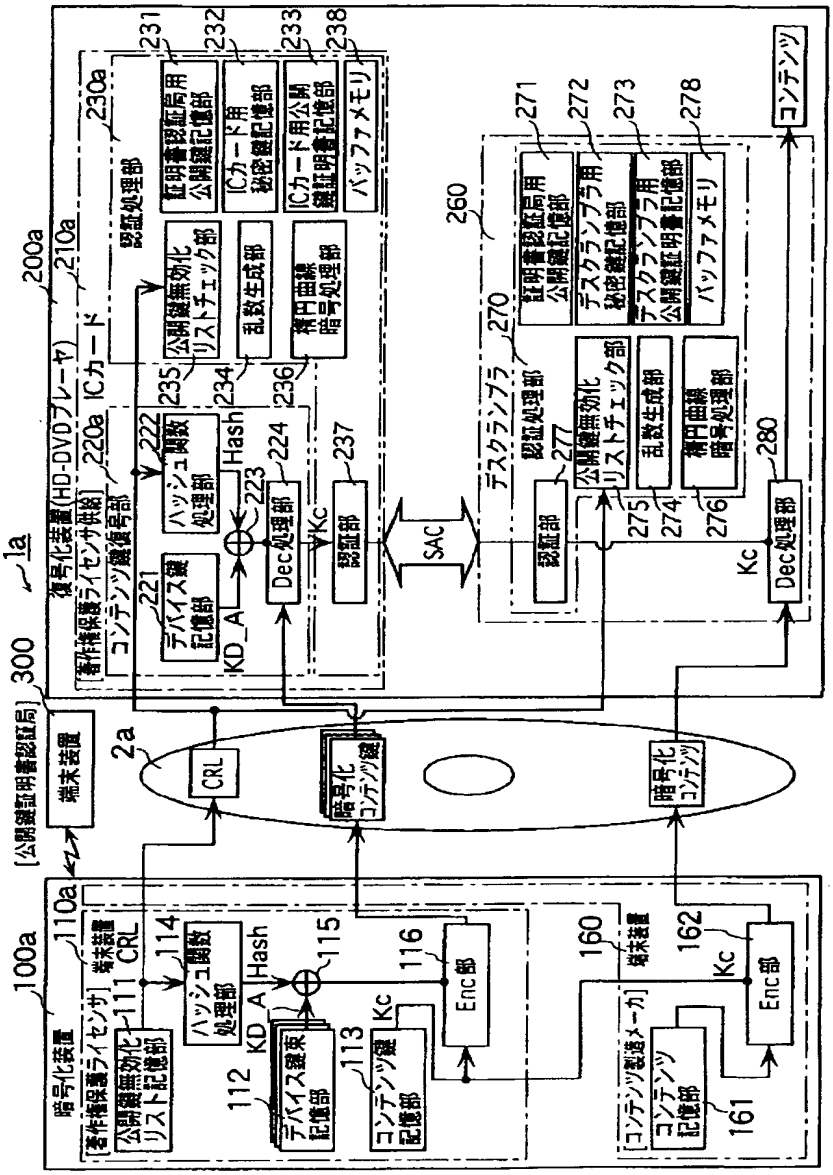
ファイルヘッダ	名前	○△□△.crl
	サイズ	79KB
	種類	証明書無効リスト
	更新日	2001/09/07/12：34
全般	バージョン	V1
	発行者	○△□△
	有効開始日	2001年09月06日
	次の更新予定日	2001年09月16日
	署名のアルゴリズム	md5RSA
無効リスト	シリアル番号	無効日
	○××…△□	2001年05月01日
	○××…○□	2000年11月29日
	⋮	⋮

【図３】

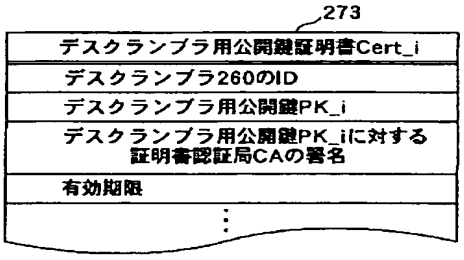
233

ICカード用用公開鍵証明書Cert_A
ICカード210のID
ICカード用公開鍵PK_A
ICカード用公開鍵PK_Aに対する証明書認証局CAの署名
有効期限
⋮

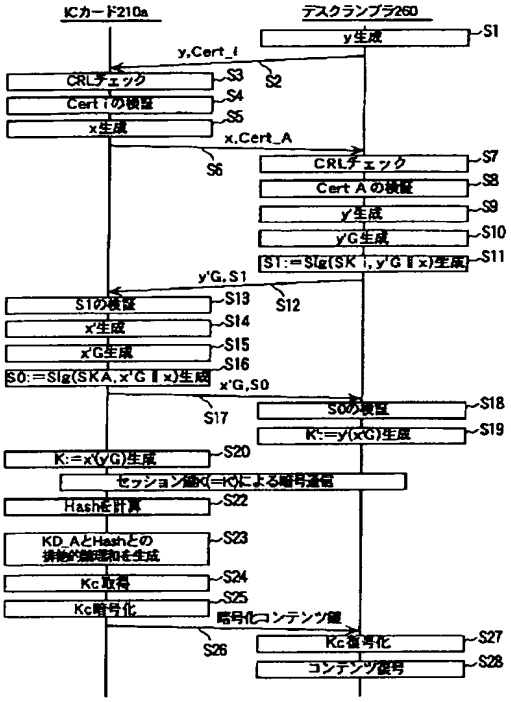
【図１】


暗号化装置
[著作権保護ライセンサ]
公開鍵無効化リスト記憶部
111
CRL
114
ハッシュ関数処理部
KD_A
Hash
115
112
デバイス鍵束記憶部
113
コンテンツ鍵記憶部
Kc
116
Enc部
110a
100a
[公開鍵証明書認証局]
端末装置
300
2a
CRL
暗号化コンテンツ鍵
暗号化コンテンツ
1a
復号化装置(HD-DVDプレーヤ)
[著作権保護ライセンサ搭載]
コンテンツ鍵復号部
221
デバイス鍵記憶部
KD_A
222
ハッシュ関数処理部
Hash
223
224
Dec処理部
Kc
237
認証部
SAC
220a
ICカード
認証処理部
231
証明書認証局用公開鍵記憶部
232
ICカード用秘密鍵記憶部
233
ICカード用公開鍵証明書記憶部
238
バッファメモリ
230a
200a
210a
235
公開鍵無効化リストチェック部
234
乱数生成部
236
楕円曲線暗号処理部
260
デスクランブラ
270
認証処理部
277
271
証明書認証局用公開鍵記憶部
272
デスクランブラ用秘密鍵記憶部
273
デスクランブラ用公開鍵証明書記憶部
278
バッファメモリ
公開鍵無効化リストチェック部
275
乱数生成部
274
楕円曲線暗号処理部
276
280
Kc
Dec処理部
コンテンツ
160
162
Kc
Enc部
[コンテンツ製造メーカ]
端末装置
コンテンツ記憶部
161

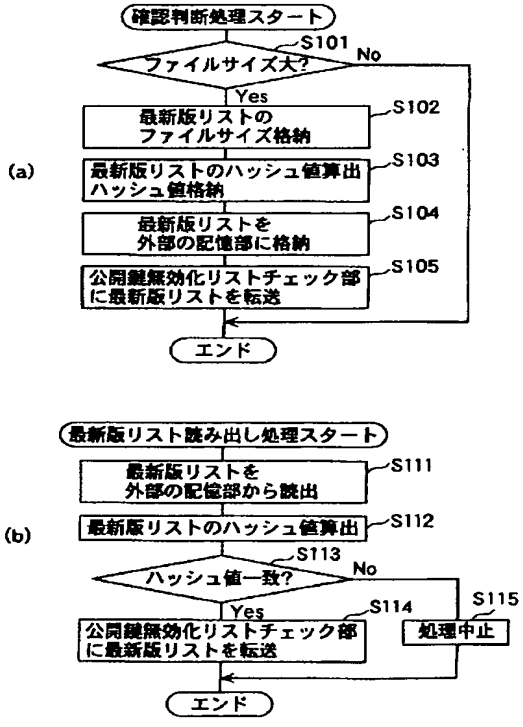
【図４】


273
デスクランブラ用公開鍵証明書Cert_i
デスクランブラ260のID
デスクランブラ用公開鍵PK_i
デスクランブラ用公開鍵PK_iに対する証明書認証局CAの署名
有効期限

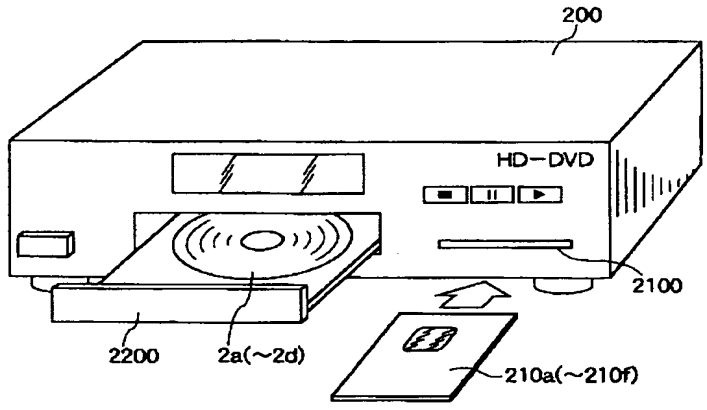
【図５】


ICカード210a
デスクランブラ260
y生成
S1
y,Cert_i
S2
CRLチェック
S3
Certiの検証
S4
x生成
S5
x,Cert_A
S6
CRLチェック
S7
Cert Aの検証
S8
y'生成
S9
y'G生成
S10
S1:=Sig(SK i,y'G‖x)生成
S11
y'G,S1
S12
S1の検証
S13
x'生成
S14
x'G生成
S15
S0:=Sig(SKA,x'G‖x)生成
S16
x'G,S0
S17
S0の検証
S18
K':=y(xG)生成
S19
K:=x(yG)生成
S20
セッション鍵K(=K')による暗号通信
Hashを計算
S22
KD_AとHashとの
排他的論理和を生成
S23
Kc取得
S24
Kc暗号化
S25
暗号化コンテンツ鍵
S26
Kc復号化
S27
コンテンツ復号
S28

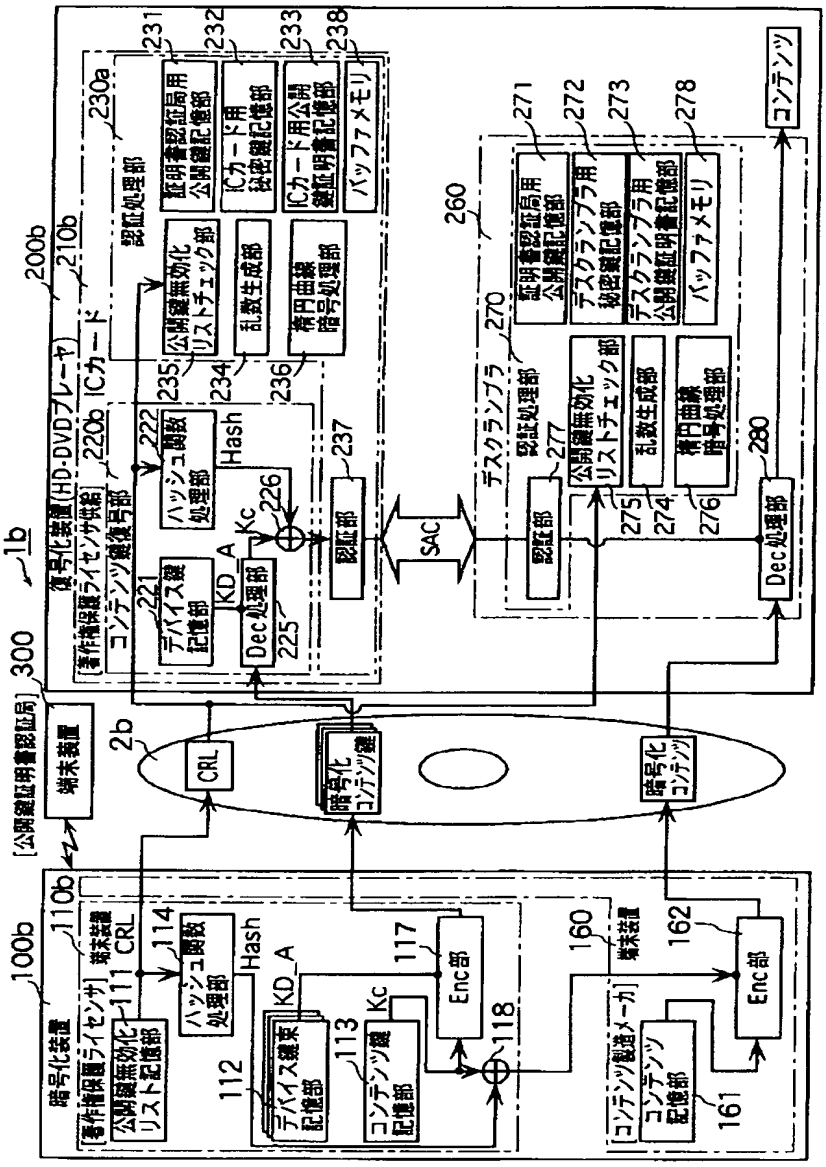
【図１１】


(a)
確認判断処理スタート
ファイルサイズ大?
S101
No
Yes
最新版リストの
ファイルサイズ格納
S102
最新版リストのハッシュ値算出
ハッシュ値格納
S103
最新版リストを
外部の記憶部に格納
S104
公開鍵無効化リストチェック部
に最新版リストを転送
S105
エンド
(b)
最新版リスト読み出し処理スタート
最新版リストを
外部の記憶部から読出
S111
最新版リストのハッシュ値算出
S112
ハッシュ値一致?
S113
No
Yes
公開鍵無効化リストチェック部
に最新版リストを転送
S114
処理中止
S115
エンド

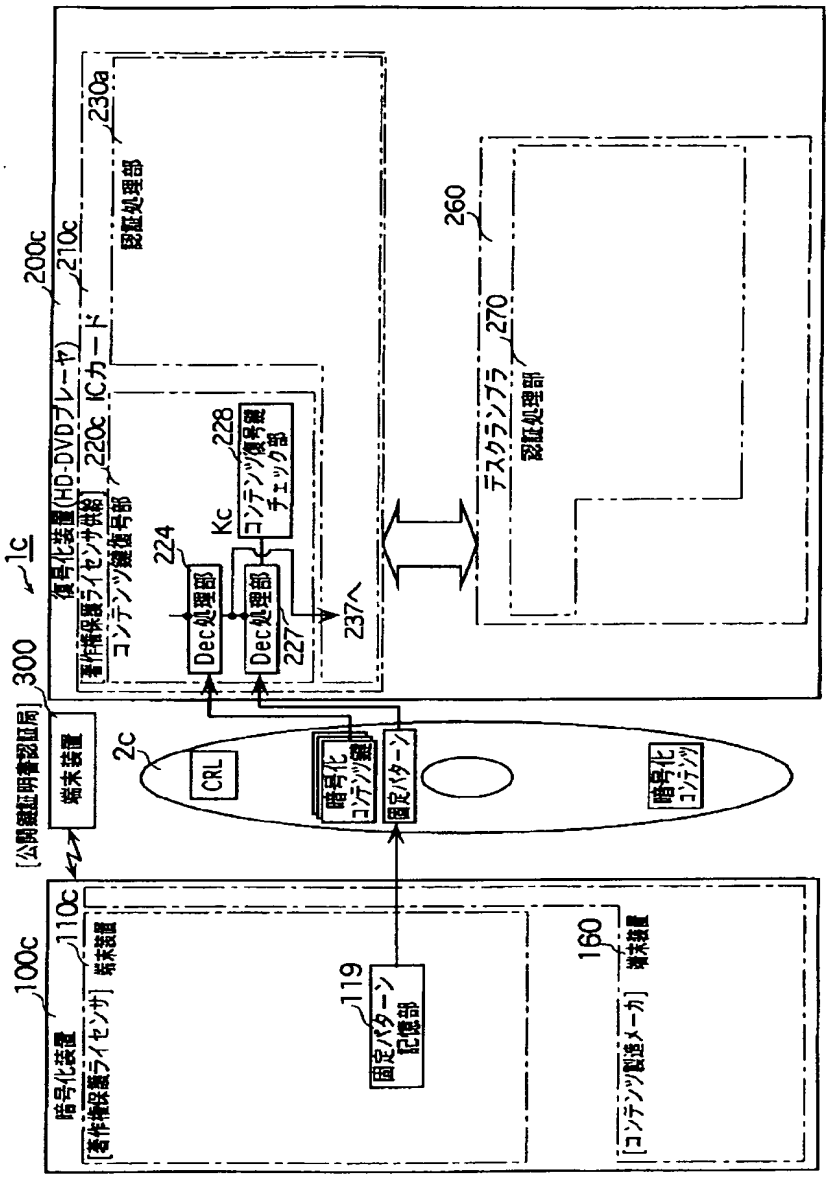
【図１２】


200
HD−DVD
2100
2200
2a(～2d)
210a(～210f)

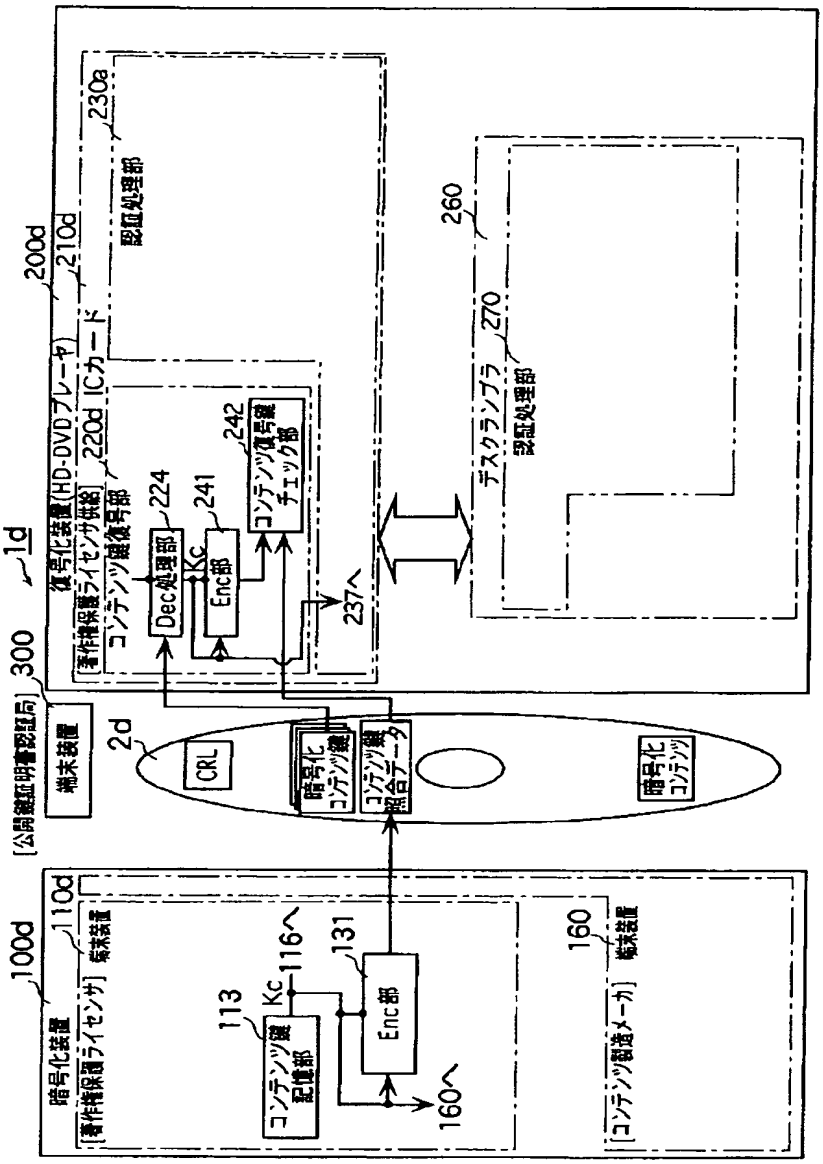
【図６】


暗号化装置
著作権保護ライセンサ
公開鍵無効化リスト記憶部
111
CRL
端末装置
110b
ハッシュ関数処理部
114
Hash
デバイス鍵記憶部
112
KD_A
コンテンツ鍵記憶部
113
Kc
Enc部
117
118
100b
160
端末装置
コンテンツ配送メーカ
コンテンツ記憶部
161
Enc部
162
[公開鍵証明書認証局]
端末装置
300
1b
2b
CRL
暗号化コンテンツ鍵
暗号化コンテンツ
復号化装置(HD-DVDプレーヤ)
著作権保護ライセンサ供給
コンテンツ復号部
220b
ICカード
210b
200b
認証処理部
230a
221
デバイス鍵記憶部
KD_A
Dec処理部
225
222
ハッシュ関数処理部
Hash
226
Kc
認証部
237
SAC
231
証明書認証局用公開鍵記憶部
232
ICカード用秘密鍵記憶部
233
ICカード用公開鍵証明書記憶部
238
バッファメモリ
235
公開鍵無効化リストチェック部
234
乱数生成部
236
楕円曲線暗号処理部
コンテンツ
260
デスクランブラ
270
認証処理部
認証部
277
271
証明書認証局用公開鍵記憶部
272
デスクランブラ用秘密鍵記憶部
273
デスクランブラ用公開鍵証明書記憶部
278
バッファメモリ
公開鍵無効化リストチェック部
275
乱数生成部
274
楕円曲線暗号処理部
276
Dec処理部
280

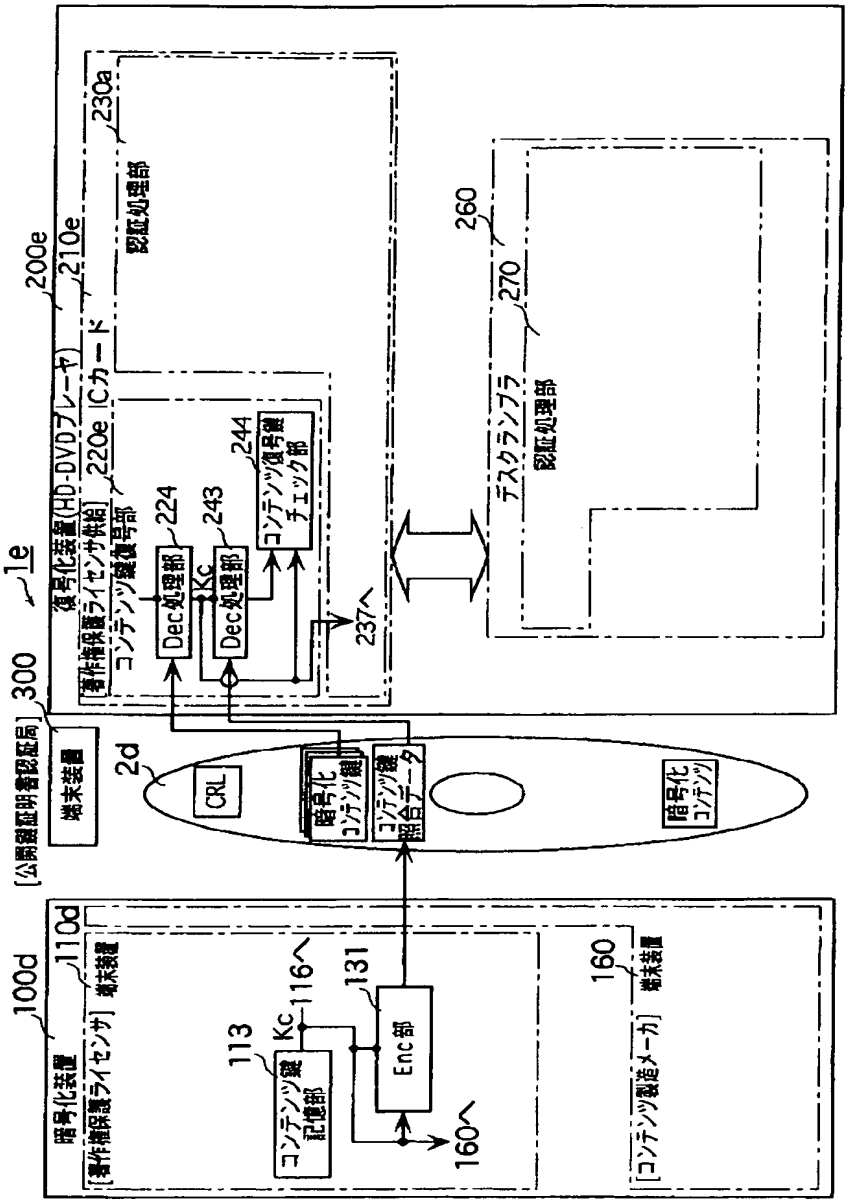
【図７】


100c
暗号化装置
[著作権保護ライセンサ]
110c
端末装置
119
固定パターン記憶部
160
[コンテンツ配送メーカ]
端末装置
[公開鍵証明書認証局]
300
端末装置
2c
CRL
暗号化コンテンツ鍵
固定パターン
暗号化コンテンツ
1c
200c
復号化装置(HD-DVDプレーヤ)
著作権保護ライセンサ供給
コンテンツ鍵復号部
220c
ICカード
210c
認証処理部
230a
224
Dec処理部
Kc
Dec処理部
227
228
コンテンツ復号鍵チェック部
237へ
260
デスクランブラ
270
認証処理部

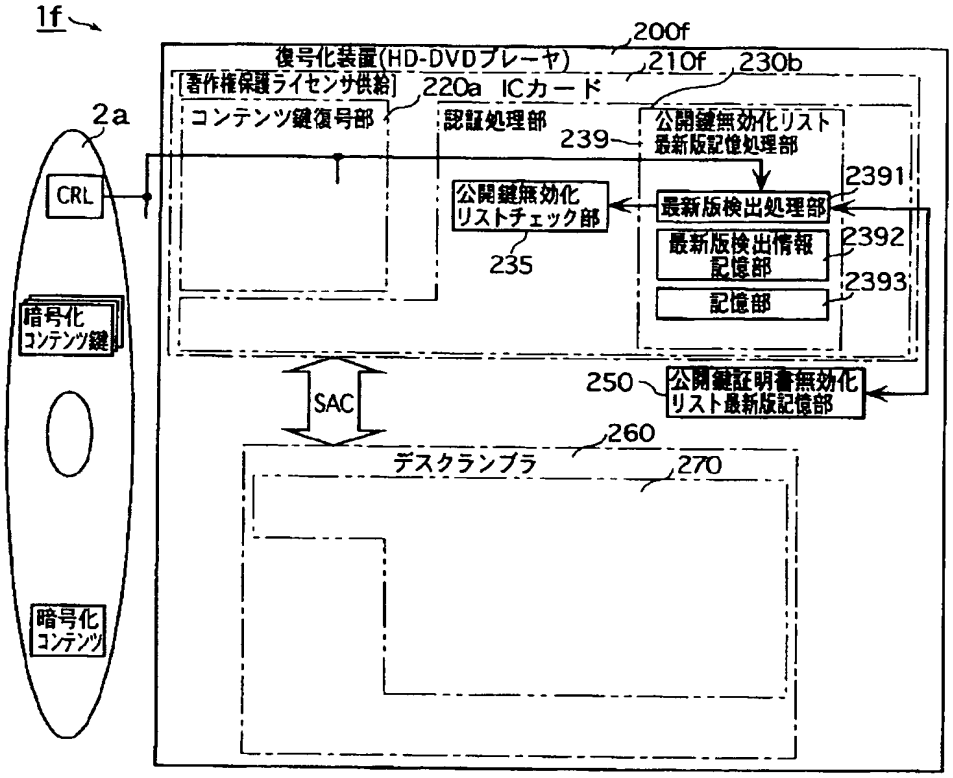
【図８】


100d
暗号化装置
[著作権保護ライセンサ]
110d
端末装置
113
コンテンツ鍵記憶部
Kc
116へ
131
Enc部
160へ
160
端末装置
[コンテンツ製造メーカ]
暗号化コンテンツ
2d
CRL
暗号化コンテンツ鍵
コンテンツ鍵照合データ
[公開鍵証明書認証局]
300
端末装置
1d
200d
復号化装置(HD-DVDプレーヤ)
210d
著作権保護ライセンサ供給
コンテンツ鍵復号部
220d ICカード
230a
認証処理部
224
Dec処理部
Kc
241
Enc部
242
コンテンツ鍵復号チェック部
237へ
260
270
デスクランブラ
認証処理部

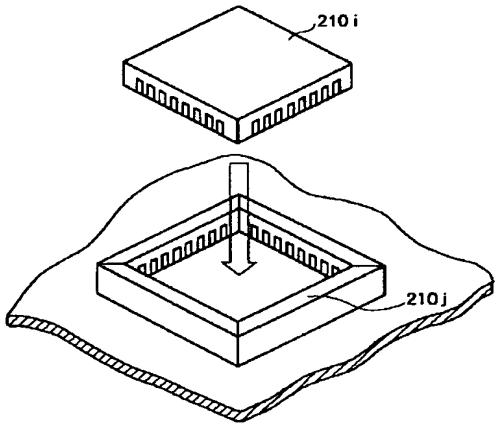
【図９】


100d
暗号化装置
[著作権保護ライセンサ]
端末装置
110d
113
Kc
コンテンツ鍵記憶部
116へ
131
Enc部
160へ
160
[コンテンツ製造メーカ]
端末装置
暗号化コンテンツ
2d
CRL
暗号化コンテンツ鍵
コンテンツ鍵照合データ
暗号化コンテンツ
[公開鍵証明書認証局]
300
端末装置
1e
200e
復号化装置(HD-DVDプレーヤ)
著作権保護ライセンサ休館
210e
220e ICカード
コンテンツ鍵復号部
224
Dec処理部
243
Kc
Dec処理部
244
コンテンツ復号鍵チェック部
237へ
認証処理部
230a
260
デスクランブラ
270
認証処理部

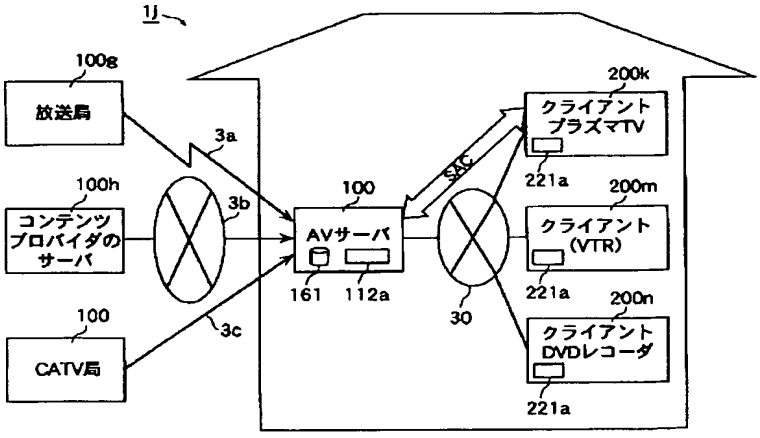
【図１０】


1f
200f
復号化装置(HD-DVDプレーヤ)
210f
230b
著作権保護ライセンス供給
220a ICカード
2a
コンテンツ鍵復号部
認証処理部
239
公開鍵無効化リスト
最新版記憶処理部
2391
CRL
公開鍵無効化
リストチェック部
最新版検出処理部
2392
最新版検出情報
記憶部
235
2393
記憶部
暗号化
コンテンツ鍵
SAC
250
公開鍵証明書無効化
リスト最新版記憶部
260
デスクランブラ
270
暗号化
コンテンツ

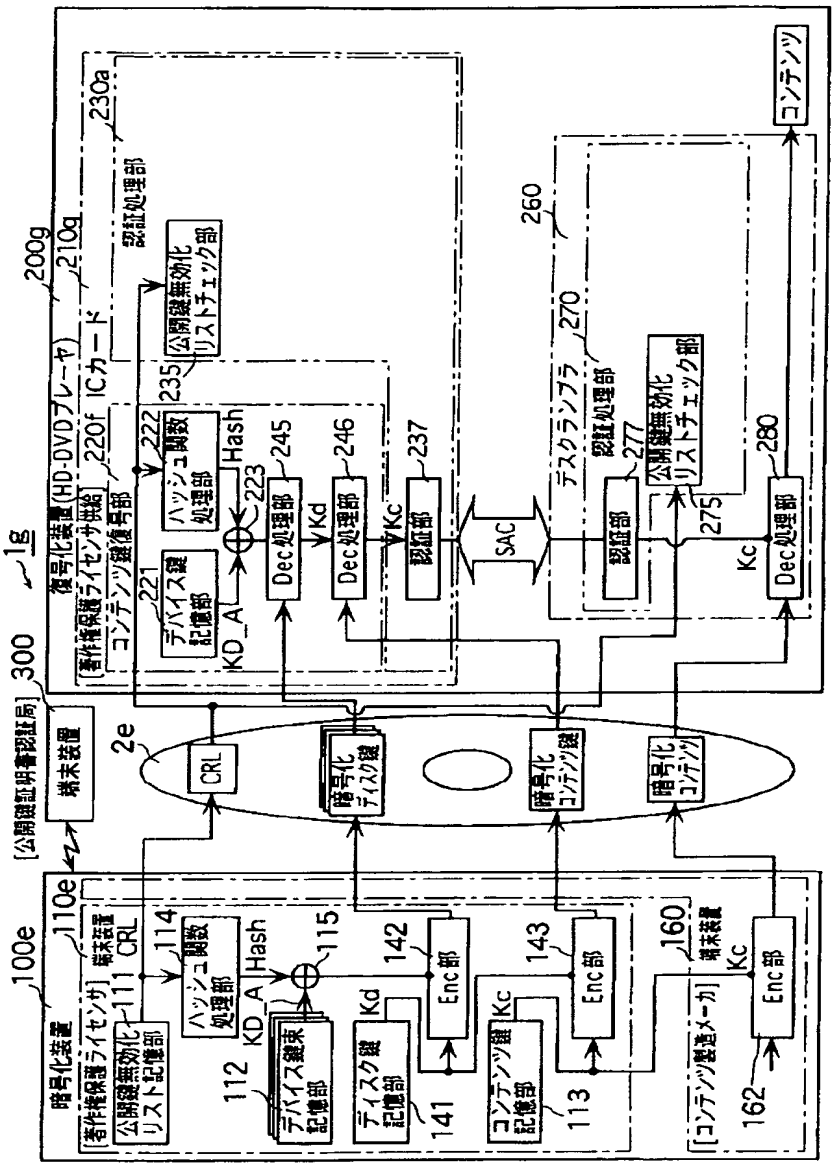
【図１６】


210i
210j

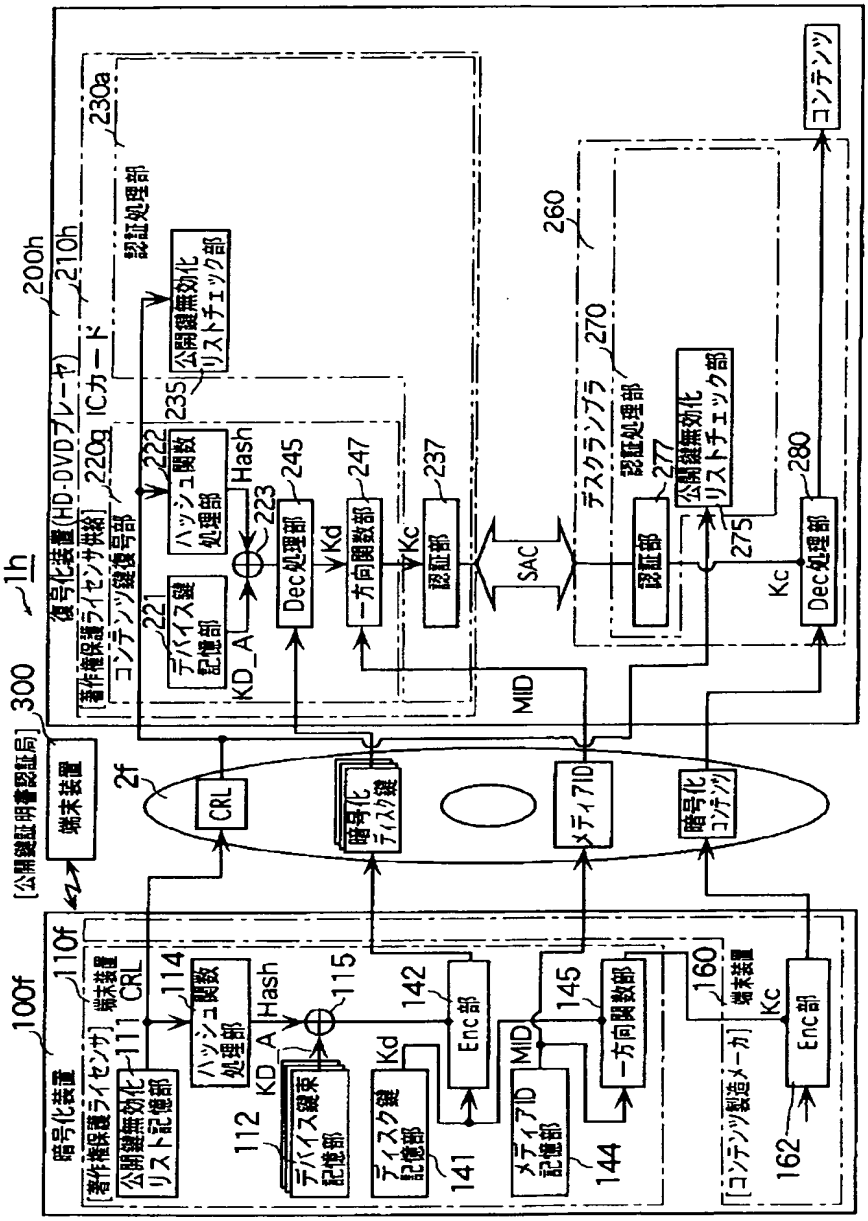
【図１７】


1j
100g
放送局
3a
200k
クライアント
プラズマTV
221a
100h
コンテンツ
プロバイダの
サーバ
3b
100
AVサーバ
200m
クライアント
(VTR)
221a
161
112a
30
100
CATV局
3c
200n
クライアント
DVDレコーダ
221a

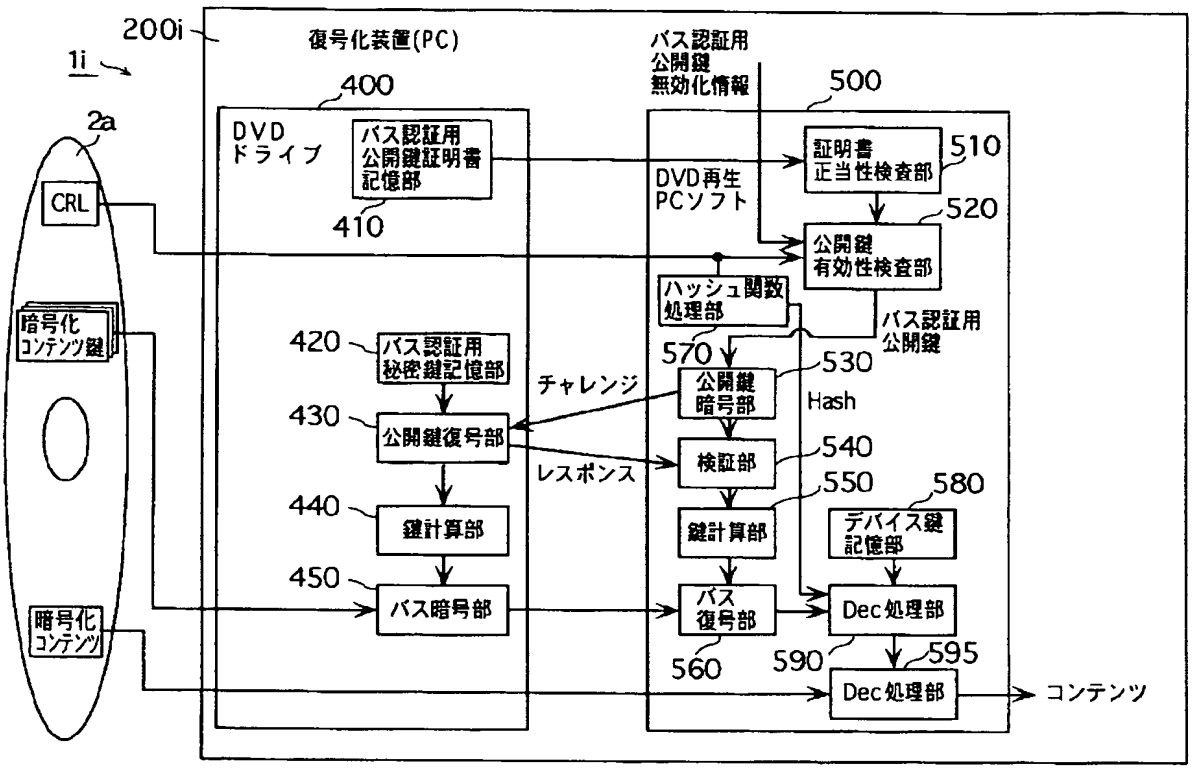
【図１３】


暗号化装置
100e
著作権保護ライセンサ
公開鍵無効化リスト記憶部
111
CRL
114
ハッシュ関数処理部
Hash
KD_A
112
デバイス鍵記憶部
115
ディスク鍵記憶部
141
Kd
142
Enc部
コンテンツ鍵記憶部
113
Kc
143
Enc部
[コンテンツ製造メーカ]
162
Kc
160
Enc部
端末装置
110e
[公開鍵証明書認証局]
300
端末装置
2e
CRL
暗号化ディスク鍵
暗号化コンテンツ鍵
暗号化コンテンツ
復号化装置(HD-DVDプレーヤ)
200g
210g
著作権保護ライセンサ
コンテンツ鍵復号部
220f
ICカード
230a
認証処理部
公開鍵無効化リストチェック部
235
ハッシュ関数処理部
222
Hash
223
デバイス鍵記憶部
221
KD_A
Dec処理部
245
Kd
Dec処理部
246
Kc
認証部
237
SAC
1g
テスクランプラ
260
認証処理部
270
認証部
277
公開鍵無効化リストチェック部
275
Kc
Dec処理部
280
コンテンツ

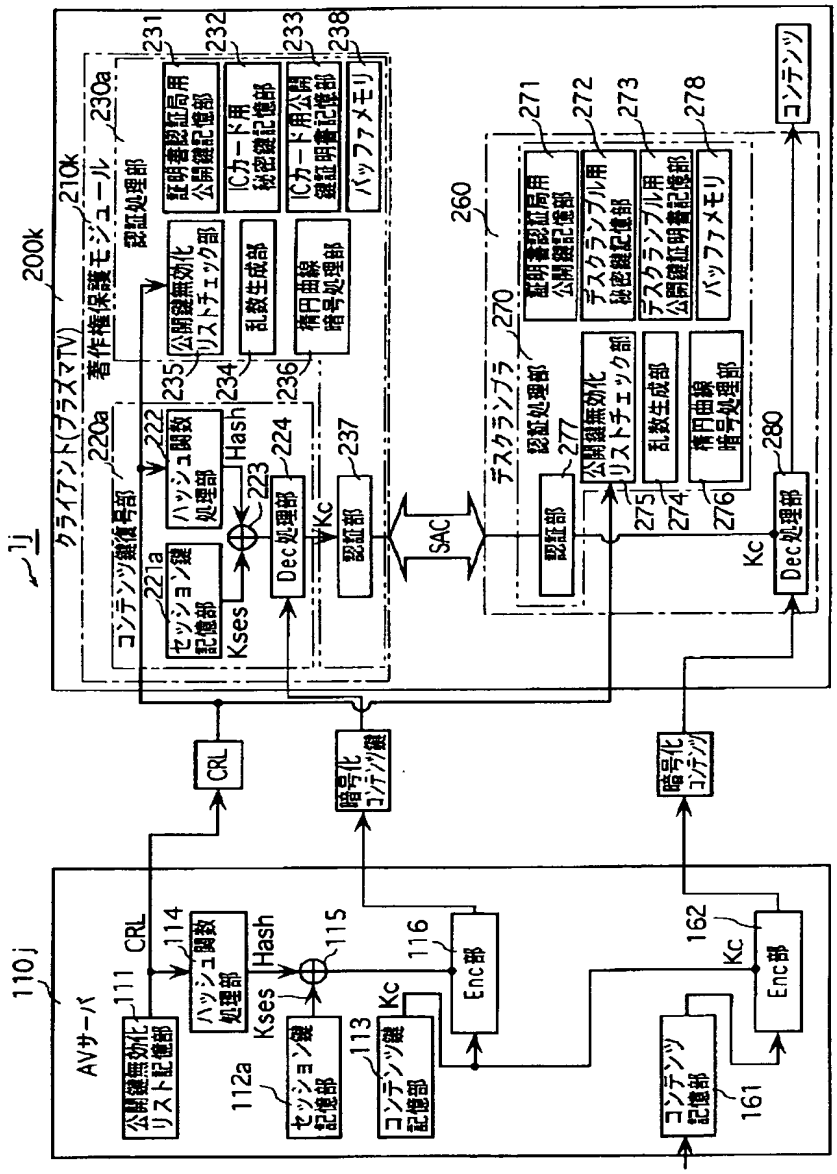
【図１４】


100f
暗号化装置
[著作権保護ライセンサ]
公開鍵無効化リスト記憶部
111
CRL
端末装置
110f
114
ハッシュ関数処理部
Hash
KD_A
112
デバイス鍵記憶部
115
Kd
ディスク鍵記憶部
141
142
Enc部
MID
メディアID記憶部
144
145
一方向関数部
160
[コンテンツ製造メーカ]
端末装置
Kc
Enc部
162
[公開鍵証明書認証局]
300
端末装置
2f
CRL
暗号化ディスク鍵
メディアID
暗号化コンテンツ
1h
復号化装置(HD-DVDプレーヤ)
[著作権保護ライセンサ]
コンテンツ鍵復号部
220g
ICカード
230a
認証処理部
公開鍵無効化リストチェック部
235
200h
210h
222
ハッシュ関数処理部
Hash
223
221
デバイス鍵記憶部
KD_A
Dec処理部
245
Kd
一方向関数部
247
Kc
認証部
237
SAC
MID
260
デスクランブラ
270
認証処理部
277
認証部
公開鍵無効化リストチェック部
275
Kc
Dec処理部
280
コンテンツ

【図１５】


200i
1i
復号化装置(PC)
バス認証用
公開鍵
無効化情報
400
500
2a
DVD
ドライブ
バス認証用
公開鍵証明書
記憶部
410
証明書
正当性検査部
510
DVD再生
PCソフト
520
公開鍵
有効性検査部
CRL
暗号化
コンテンツ鍵
ハッシュ関数
処理部
バス認証用
公開鍵
420
バス認証用
秘密鍵記憶部
570
530
公開鍵
暗号部
チャレンジ
Hash
430
公開鍵復号部
検証部
540
レスポンス
550
580
440
鍵計算部
鍵計算部
デバイス鍵
記憶部
450
暗号化
コンテンツ
バス暗号部
バス
復号部
Dec処理部
560
590
595
Dec処理部
コンテンツ

【図１８】



フロントページの続き

(51) Int. Cl.[7]	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
		H04L 9/00	675D

(72)発明者　永井　隆弘
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　石原　秀志
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム(参考) 5B017 AA03 BA07 CA09 CA16
5J104 AA07 AA08 AA12 AA16 EA05
EA18 JA01 JA03 JA21 JA31
KA02 KA05 KA15 LA01 LA03
LA06 NA02 NA35 NA37 NA38
NA40 NA41 NA42

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☑ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.